[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/14
G06F 12/16

[12]发明专利申请公开说明书

[21]申请号 02105432.0

[43]公开日 2002年9月25日

[11]公开号 CN 1371056A

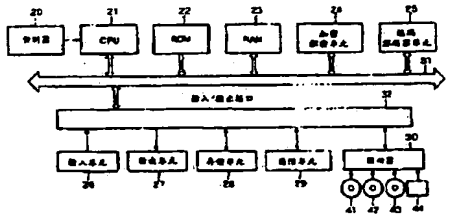
[22]申请日 2002.2.9 [21]申请号 02105432.0
[30]优先权
[32]2001.2.9 [33]JP [31]33114/01
[32]2001.3.29 [33]JP [31]94803/01
[71]申请人 索尼公司
地址 日本东京都
[72]发明人 田中浩一 河上达
黑田寿祐 石黑隆二
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 张志醒

权利要求书4页 说明书41页 附图页数44页

[54]发明名称 信息处理方法/装置和程序

[57]摘要

客户机从内容服务器接收加密的内容。内容的首部包括用于识别使用内容 所需要的许可的许可识别信息。客户机请求许可服务器发送由许可识别信息所 识别的许可。当接收到对许可的请求时,许可服务器在向客户机发送许可之前 执行收费处理。客户机保存从许可服务器接收的许可。保存的许可作为加密和 播放内容的条件。结果,内容能够以高自由度分配并只有授权的用户能够使用 内容。



ISSN1008-4274

知识产权出版社出版

02.03.12

权 利 要 求 书

1．一种信息处理装置，它允许通过需要使用该内容的许可来使用内容，所述的信息处理装置包括：

内容存储装置，用于存储指定使用所述内容时所述用户要求的所述许可的许可指定信息、所述内容的加密数据和对所述内容的所述加密数据解密所要求的密钥信息；

许可存储装置，用于存储包括用于指定所述内容的内容指定信息的所述许可，该内容的使用是被允许的；

判断装置，用于形成所述用户使用所述内容时所要求的所述许可是否已经存储在所述许可存储装置中的判断；和

解密装置，它用来在由所述判断装置形成的所述判断的结果表明用户使用所述内容时所要求的所述许可已经存储在所述许可存储装置中的条件下，解密所述内容的所述加密数据。

2．按照权利要求 1 的信息处理装置，还包括：

发送装置，用于将包括所述许可识别信息的许可请求发送到许可服务器，该许可识别信息用于识别所述用户使用所述内容时要求的所述许可；和

接收装置，用于接收许可服务器发送的所述许可，

其中，所述接收装置接收的所述许可存储在所述许可存储装置中。

3．按照权利要求 1 的信息处理装置，还包括再现装置，用于再现由所述解密装置解密的所述内容数据，其中所述内容的所述数据是文本数据、图像数据、音频数据、动画数据或以上这些数据的组合。

4．按照权利要求 1 的信息处理装置，还包括设备节点密钥存储装置，用于存储设备节点密钥，其中：

所述密钥信息包括 EKB（使能密钥块）；以及

所述解密装置通过使用存储在所述设备节点密钥存储装置中的所述设备节点密钥解密所述 EKB（使能密钥块），并通过使用作为所述 EKB 解密结果的获得的根密钥解密所述内容数据。

5．按照权利要求 4 的信息处理装置，其中：

所述密钥信息还包括通过使用所述 EKB（使能密钥块）的所述根密钥加密

的内容密钥；

所述内容的所述数据通过使用所述内容密钥来加密，；以及

所述解密装置对通过使用作为所述 EKB（使能密钥块）的解密结果获得的所述根密钥解密由所述内容密钥加密的所述内容数据，EKB（使能密钥块）通过使用存储在所述设备节点密钥存储装置中的所述设备节点密钥来解密。

6．按照权利要求 1 的信息处理装置，其中所述许可还包括表示使用所述内容的条件的使用条件信息，该内容的使用由所述许可所允许。

7．按照权利要求 1 的信息处理装置，其中所述许可还包括通过使用许可服务器的密钥指示的电子签名。

8．按照权利要求 2 的信息处理装置，还包括终端 ID 存储装置，用于存储识别所述信息处理装置的终端指定信息；

所述发送装置发送的所述许可请求还包括存储在所述终端 ID 存储装置中的所述终端识别信息；

所述接收装置接收的所述许可包括终端 ID；以及

所述判断装置比较包括在所述许可中的所述终端识别信息和存储在所述终端 ID 存储装置中的所述终端识别信息，并只有在包括在所述许可中的所述终端识别信息与存储在所述终端 ID 存储装置中的所述终端识别信息相匹配时，确定所述接收装置接收的所述许可是允许所述内容使用的许可。

9．一种信息处理方法，它用于通过要求用户具有使用该内容的许可来允许所述用户使用用户请求的内容，所述信息处理方法包括：

内容存储步骤，存储用于指定所述用户使用所述内容时所要求的所述许可的许可指定信息、所述内容的加密数据和对所述加密的所述内容数据解密所要求的密钥信息；

许可存储步骤，存储包括用于指定所述内容的内容指定信息的所述许可，该内容的使用由许可所允许；

判断步骤，形成对所述用户使用所述内容所要求的所述许可是否已经存储在所述许可存储装置中的判断；和

解密步骤，在该步骤中在所述判断装置形成的所述判断结果表明用户使用所述内容时所要求的所述许可已经存储在所述许可存储装置中的条件下，所述内容的所述加密数据被解密。

02.09.12

10．一种由计算机执行的程序，它用于通过要求用户具有使用该内容的许可来执行允许用户使用内容的处理，所述程序包括：

内容存储步骤，存储用于指定所述用户使用所述内容时所要求的所述许可的许可指定信息、所述内容的加密数据和对所述加密的所述内容数据解密所要求的密钥信息；

许可存储步骤，存储包括用于指定所述内容的内容指定信息的所述许可，该内容的使用由该许可所允许；

判断步骤，形成对用户使用所述内容所要求的所述许可是否已经存储在所述许可存储装置中的判断；和

解密步骤，在该步骤中在所述判断装置形成的判断结果表明所述用户使用所述内容时所要求的所述许可已经存储在所述许可存储装置中的条件下，所述内容的所述加密数据被解密。

11．按照权利要求10的程序，所述程序或所述程序的一部分是加密的。

12．一种许可服务器，用于发出允许内容使用的许可，所述许可服务器包括：

许可存储装置，用于保存所述许可，许可包括：

用于指定所述内容的内容指定信息，该内容的使用由该许可所允许；和

用于识别信息处理装置的终端识别信息；

接收装置，用于从所述信息处理装置中接收包括用于识别所述许可的许可识别信息的许可请求；

提取装置，用于从所述许可存储装置中提取由包括在所述许可请求中的所述许可识别信息识别的所述许可；

处理装置，用于把所述终端识别信息加入到由所述提取装置提取的所述许可中；

签名装置，用于把签名放到所述许可中，该许可包括由所述处理装置通过使用许可服务器的密钥加入的所述终端识别信息；和

发送装置，用于向所述信息处理装置发送带有由所述签名装置放入其中的所述签名的许可，所述许可请求从信息处理装置接收。

13．一种信息处理方法，它用于发出允许使用内容的许可，所述信息处理方法包括：

许可存储步骤，存储所述的许可，许可包括：

用于指定所述内容的内容指定信息，该内容的使用由许可所允许；和

用于识别信息处理装置的终端识别信息；

接收步骤，用于从所述信息处理装置中接收包括用于识别所述许可的许可识别信息的许可请求；

提取步骤，提取存储在所述许可存储装置中并由包括在所述许可请求中的许可识别信息识别的许可；

处理步骤，把所述终端识别信息加入到在所述提取步骤提取的所述许可中；

签名步骤，把签名放到所述许可中，其中许可包括在所述处理步骤通过使用用在所述信息处理方法中的许可服务器的密钥加入的所述终端识别信息；和

发送步骤，发送带有在所述签名步骤放入其中的所述签名的所述许可到所述信息处理装置中，所述许可请求从信息处理装置接收。

14．一种由计算机执行的程序，用于执行发出允许使用内容的许可的处理，所述程序包括：

许可存储步骤，存储所述的许可，该许可包括：

用于指定所述内容的内容指定信息，该内容指定信息的使用由许可所允许；和

用于识别信息处理装置的终端识别信息，

接收步骤，用于从所述信息处理装置中接收包括用于识别所述许可的许可识别信息的许可请求；

提取步骤，提取存储在所述许可存储装置中并由包括在所述许可请求中的许可识别信息识别的许可；

处理步骤，把所述终端识别信息加入到在所述提取步骤提取的所述许可中；

签名步骤，把签名放到所述许可中，其中许可包括在所述处理步骤通过使用用在所述信息处理方法中的许可服务器的密钥加入的所述终端识别信息；和

发送步骤，发送带有在所述签名步骤放入其中的所述签名的所述许可到所述信息处理装置中，所述许可请求从信息处理装置接收。

02.03.12

说　　明　　书

信息处理方法/装置和程序

技术领域

总的来说，本发明涉及一种信息处理方法、信息处理装置、程序存储介质和程序。尤其是，本发明涉及一种用于防止未经内容版权所有人许可非法复制和使用该内容的信息处理方法和信息处理装置，执行该信息处理方法的程序和存储该程序的程序存储介质。

背景技术

近年来，在通过互联网允许多个用户免费交换音乐数据的内容交换系统中，一个用户向其他用户提供他自己拥有的音乐数据并从其他用户接收他所没有的音乐数据。

从而在这样的内容交换系统中，一个用户拥有的音乐或其他内容能够由其他用户所欣赏。因此，很多用户就不需要购买这首音乐或这个内容。结果，由于这首音乐或这个内容销售得不好，内容版权的所有者失去了伴随着这首音乐或这个内容的销售由这首音乐或这个内容的使用获得版税的机会。

因此，在社会上有防止内容被复制和非法使用的要求。

发明内容

因此，本发明的一个目的是针对上述问题可靠地防止内容被非法使用。

按照本发明的一个方面，提供一种信息处理装置，它允许通过需要使用该内容的许可来使用内容。信息处理装置包括：

内容存储装置，用于存储指定使用内容时用户要求的许可的许可指定信息、内容的加密数据和对内容的加密数据解密所要求的密钥信息；

许可存储装置，用于存储包括用于指定内容的内容指定信息的许可，该内容的使用是被允许的；

判断装置，用于形成对用户使用内容时所要求的许可是否已经存储在许可存储装置中的判断；和

解密装置，它用来在由判断装置形成的判断的结果表明用户使用内容时所要求的许可已经存储在许可存储装置中的条件下，解密该内容的加密数据。

信息处理装置还包括发送装置和接收装置，发送装置用于发送包括许可识别信息的许可请求，该许可识别信息用于识别用户使用内容时所要求的许可，接收装置用于接收许可服务器发送的许可。另外，接收装置接收的许可存储在许可存储装置中。

信息处理装置还包括再现装置，用于再现由解密装置解密的内容数据，其中内容数据是文本数据、图像数据、音频数据、动画数据或以上这些数据的结合。

信息处理装置还包括设备节点密钥存储装置，用于存储设备节点密钥。密钥信息包括 EKB（使能密钥块）。解密装置通过使用存储在设备节点密钥存储装置中的设备节点密钥解密 EKB（使能密钥块），并通过使用作为 EKB 解密结果的获得的根密钥解密内容数据。

在信息处理装置中，密钥信息还包括通过使用 EKB（使能密钥块）的根密钥加密的内容密钥。内容数据通过使用内容密钥来加密。解密装置对通过使用作为 EKB（使能密钥块）的解密结果获得的根密钥的内容密钥加密的内容数据解密，EKB（使能密钥块）通过使用存储在设备节点密钥存储装置中的设备节点密钥来解密。

信息处理装置中，许可还包括表示使用内容的条件的使用条件信息，该信息的使用由许可所允许。

信息处理装置中，许可还包括通过使用许可服务器的密钥签发的一个电子签名。

信息处理装置还有终端 ID 存储装置，用于存储识别信息处理装置的终端指定信息。发送装置发送的许可请求还包括存储在终端 ID 存储装置中的终端 ID。接收装置接收的许可包括终端 ID。判断装置比较包括在许可中的终端识别信息和存储在终端 ID 存储装置中的终端识别信息，并只有在包括在许可中的终端 ID 与存储在终端 ID 存储装置中的终端识别信息相匹配时，确定接收装置接收的许可是允许内容使用的许可。

按照本发明的另一方面，提供一种信息处理方法，它用于通过要求用户具有使用该内容的许可来允许用户使用用户请求的内容。信息处理方法包括：

内容存储步骤，存储用于指定用户使用内容时所要求的许可的许可 ID、内容的加密数据和对加密的内容数据解密所要求的密钥信息；

02.03.12

许可存储步骤，存储包括用于指定内容的内容指定信息，该内容的使用由许可所允许；

判断步骤，形成对用户使用内容所要求的许可是否已经存储在许可存储装置中的判断；和

解密步骤，在该步骤中在判断装置形成的判断结果表明用户使用内容时所要求的许可已经存储在许可存储装置中的条件下，内容的加密数据被解密。

按照本发明的再另一方面，提供一种由计算机执行的程序，它用于通过要求用户具有使用该内容的许可来执行允许用户使用内容的处理。该程序包括：

内容存储步骤，存储用于指定用户使用内容时所要求的许可的许可指定信息、内容的加密数据和对加密的内容数据解密所要求的密钥信息；

许可存储步骤，存储包括用于指定内容的内容指定信息，该内容的使用由许可所允许；

判断步骤，形成对用户使用内容所要求的许可是否已经存储在许可存储装置中的判断；和

解密步骤，在该步骤中在判断装置形成的判断结果表明用户使用内容时所要求的许可已经存储在许可存储装置中的条件下，内容的加密数据被解密。

程序或程序的一部分是加密的。

仍然按照本发明的再一方面，提供一种许可服务器，用于发出允许内容使用的许可。许可服务器包括：

用于存储许可的许可存储装置，其中许可包括：

用于指定内容的内容指定信息，该信息的使用由许可所允许；和

用于识别信息处理装置的终端识别信息；

接收装置，用于从信息处理装置中接收包括用于识别许可的许可识别信息的许可请求；

提取装置，用于提取由包括在来自许可存储装置中的许可请求中的许可识别信息识别的许可；

处理装置，用于把终端识别信息加入到由提取装置提取的许可中；

签名装置，用于把一个签名放到许可中，该许可包括由处理装置通过使用许可服务器的密钥加入的终端识别信息；和

发送装置，用于向信息处理装置发送带有由签名装置放入其中的签名的许

可，许可请求从信息处理装置接收。

仍然按照本发明的另一方面，提供另一种信息处理方法，它用于发出允许使用内容的许可。另一种信息处理方法包括：

许可存储步骤，存储包括指定内容的内容指定信息和用于识别信息处理装置的终端识别信息的许可，该内容指定信息的使用由许可所允许；

接收步骤，从信息处理装置中接收包括用于识别许可的许可识别信息的许可请求；

提取步骤，提取存储在许可存储装置中的许可和由包括在许可请求中的许可识别信息识别的许可；

处理步骤，把终端识别信息加入到在提取步骤提取的许可中；

签名步骤，把签名放到许可中，其中许可包括在处理步骤通过使用用在信息处理方法中的许可服务器的密钥加入的终端识别信息；和

发送步骤，发送带有在签名步骤放入其中的签名的许可到信息处理装置中，该许可请求从信息处理装置接收。

还按照本发明的另一方面，提供另一种由计算机执行的程序，用于执行发出允许使用该内容的许可的处理。另一个程序包括：

许可存储步骤，存储包括指定内容的内容指定信息和用于识别信息处理装置的终端识别信息的许可，该内容指定信息的使用由许可所允许；

接收步骤，从信息处理装置中接收包括用于识别许可的许可识别信息的许可请求；

提取步骤，提取存储在许可存储装置中的许可和由包括在许可请求中的许可识别信息识别的许可；

处理步骤，把终端识别信息加入到在提取步骤提取的许可中；

签名步骤，把签名放到许可中，其中许可包括在处理步骤通过使用用在信息处理方法中的密钥加入的终端识别信息；和

发送步骤，发送带有在签名步骤放入其中的签名的许可到信息处理装置中，该许可请求从信息处理装置接收。

在本发明提供的信息处理方法、信息处理装置和程序中，在用户具有使用内容的许可的条件下，内容被解密并能够被使用。

在本发明提供的许可服务器和信息处理装置中，有效的许可只发送到特定

信息处理装置。

附图说明

图 1 是表示采用本发明应用的内容交换系统结构的框图；

图 2 是表示图 1 中示出的客户机结构的框图；

图 3 是用于解释由图 1 所示的客户机执行的下载内容的处理的流程图；

图 4 是用于解释由图 1 所示的客户机执行的向客户提供内容的处理的流程图；

图 5 是表示在图 4 中示出的流程图步骤 S26 产生的数据的典型格式图；

图 6 是用来解释由图 1 所示的客户机执行的播放内容的处理的流程图；

图 7 是用来解释图 6 所示流程图中步骤 S43 执行的获取许可处理细节的流程图；

图 8 是许可的结构图；

图 9 是用来解释由图 1 所示的许可服务器执行的发送许可的处理的流程图；

图 10 是用来解释图 6 所示的流程图中的步骤 S45 执行的更新许可处理细节的流程图；

图 11 是用来解释由图 1 所示的许可服务器执行的更新许可处理流程图；

图 12 是表示密钥结构的解释性的图；

图 13 是表示分类节点的解释性的图；

图 14 是具体表示节点与设备典型结合的图；

图 15A 和 15B 是表示 EKB（使能密钥块）结构的解释性的图；

图 16 是表示 EKB（使能密钥块）使用的解释性的图；

图 17 是表示 EKB（使能密钥块）的典型格式的解释性的图；

图 18A 至 18C 是表示在一个 EKB（使能密钥块）中标记结构的解释性的图；

图 19 是表示通过使用 DNK（设备节点密钥）解密内容的处理的解释性的图；

图 20 是表示典型的 EKB（使能密钥块）的图；

图 21 是表示多个内容分配到设备的解释性的图；

图 22 是表示许可类别的解释性的图；

图 23 是用来解释由客户机执行的分割步骤的流程图；

图 24 是表示水印结构的解释性的图；

图 25 是表示内容的典型结构的解释性的图；

图 26 是表示公开的密钥的典型证明的图；

图 27 是表示内容分配的解释性的图；

图 28 是用来解释由客户机执行的检测内容的处理的流程图；

图 29 是表示典型的通过使用标记跟踪 EKB（使能密钥块）的解释性的图；

图 30 是表示典型的 EKB（使能密钥块）结构的图；

图 31 是表示标记结构的解释性的图；

图 32 是用来解释由客户机执行的购买许可的处理的流程图；

图 33 是用来解释由客户服务器执行的购买许可的处理的流程图；

图 34 是表示标记结构的解释性的图；

图 35 是用来解释由客户机执行的为客户的证明分类的处理的流程图；

图 36 是用来解释由内容服务器执行的分类证明的处理的流程图；

图 37 是表示典型的一组证明的图；

图 38 是用来解释由内容服务器执行的形成组的处理的流程图；

图 39 是表示典型的加密内容密钥的处理的图；

图 40 是用来解释由属于一组的客户机执行的处理的流程图；

图 41 是用来解释由客户机执行的检测对另一个客户机的许可的处理的流程图；

图 42 是用来解释由客户机执行的接收由另一个客户机从其他客户机检测出的许可的的处理的流程图；

图 43 是用来解释由客户机执行的播放在另一个客户机检出的许可的处理的流程图；

图 44 是用来解释由客户机执行的登记由另一个客户机检出许可的处理流程图；

图 45 是表示由客户机执行的发出请求进行将一个许可登记到另一个客户机的处理从而执行由图 44 所示的流程图表示的许可检测处理；

图 46 是表示 MAC（消息验证码）产生的解释性的图；

图 47 是用来解释解密 ICV（完整性检测值）产生密钥处理的流程图；

图 48 是用来解释解密 ICV 产生密钥的其他处理的流程图；

图 49A 和 49B 是表示基于 ICV 的复制许可操作管理的解释性的图；

图 50 是表示许可管理的解释图。

具体实施方式

图 1 是表示采用本发明应用的内容交换系统的结构框图。客户机 1-1 和 1-2 连接到互联网 2。在随后的描述中，如果不必相互区分客户机 1-1 和 1-2，则客户机 1-1 和 1-2 每个都用通用的附图标记 1 来表示。在该实施例中，只示出了两个客户机。然而，任意数量的客户机都可以连接到互联网 2。

另外，内容服务器 3、许可服务器 4 和收费服务器 5 也连接到互联网 2。内容服务器 3 向客户机 1 提供内容，许可服务器提供给客户机 1 使用内容服务器 3 提供的内容所要求的许可。当客户机 1 从许可服务器 4 接收许可时，收费服务器 5 执行收费程序。

任意数量的内容服务器 3、许可服务器 4 和收费服务器 5 能够连接到互联网 2。

图 2 是表示客户机 1 的结构的框图。

在图 2 中示出的客户机 1 中，CPU（中央处理器）21 按照存储在 ROM（只读存储器）22 中的程序和从存储单元 28 装入到 RAM（随机读取存储器）23 的程序执行各种处理。计时器 20 测量持续时间并把测量结果送到 CPU 21。RAM 23 也用来存储执行各种处理时 CPU 21 所需要的数据。

加密和解密单元 24 对内容加密并对已经加密的内容解密。编码解码器单元 25 按照 ATRAC（自适应转换声音编码）-3 系统将内容编码并把编码的内容送到半导体存储器 44 存储在其中。半导体存储器 44 通过输入/输出接口 32 连接到驱动器 30。另外，编码解码器单元 25 对通过驱动器 30 从半导体存储器 44 读出的编码后的数据解码。

半导体存储器 44 的一个例子是记忆棒（一个商标标志）。

CPU21、ROM22、RAM23、加密和解密单元 24 和编码解码器 25 通过总线 31 互相连接。总线 31 也连接到输入/输出接口 32。

输入/输出接口 32 连接到输入单元 26、输出单元 27、存储单元 28 和通信单元 29。输入单元 26 包括键盘和鼠标。输出单元 27 包括扬声器和比如 CRT 或 LCD 的显示单元。通信单元 29 包括调制解调器和终端适配器。通信单元 29

通过互联网 2 执行通信。更特殊的是，通信单元 29 和其他客户机之间交换模拟和数字信号。

如果需要，输入/输出接口 32 也连接到驱动器 30，在驱动器上装配有适当的存储介质，比如磁盘 41、光盘 42、磁光盘 43 或半导体存储器 44。如果需要，计算机程序能够从存储介质中读出并安装在存储单元 28 中。

内容服务器 3、许可服务器 4 和收费服务器 5 的结构在图中示出。然而，内容服务器 3、许可服务器 4 和收费服务器 5 每个都是带有图 2 中的客户机 1 基本同样结构的计算机。为此，图 2 的结构中示出的一些附图标记在随后的描述中用来表示使用在内容服务器 3、许可服务器 4 和收费服务器 5 中的相同部分。

通过参考图 3 所示的流程图，接下来的描述解释从内容服务器 3 向客户机 1 提供内容的过程。

如图中所示，流程开始于步骤 S1，在该步骤中用户通过操作输入单元 26 键入命令接入内容服务器 3。按照该命令，CPU21 控制通信单元 29 通过互联网 2 接入到内容服务器 3。接着，在下一个步骤 S2，当用户通过操作输入单元 26 指定想要的内容时，CPU21 接受该指定。通信单元 29 通过互联网 2 通知内容服务器 3 该指定内容。被告知指定内容后，如同将要描述的那样，在图 4 所示流程图表示中，内容服务器 3 发送被编码的内容的数据。接着，在下一个步骤 S3，CPU21 通过通信单元 29 接收内容。随后，在下一个步骤 S4，内容编码数据存储在存储单元 28 的硬盘中。

参照图 4 所示流程图，接下来的描述解释了在步骤 S2 中由内容服务器 3 执行的发送客户机 1 请求内容的处理。应当注意到，因为内容服务器 3 具有包括与客户机 1 中所使用的相同部件的结构，所以与图 2 中示出的那些附图标记相同的附图标记用来表示在接下来的描述中相同的部件。

如图 4 所示，流程开始于步骤 S21，在该步骤中，使用在内容服务器 3 中的 CPU21 等待通过通信单元 29 从互联网 2 到来的接入。当确认接入已经到达时，程序的流程进行到步骤 S22，在该步骤中，获取由客户机 1 发送以指定内容的信息。在图 3 所示的流程图中的步骤 S2 中，指定内容的信息由客户机 1 发送。

接着，在下一个步骤 S23，内容服务器 3 使用的 CPU21 读出在步骤 S22 从

存储单元 28 获取的信息所指定的内容。从存储单元 28 读出的内容是从存储单元 28 中存储的内容中选择出来的。接着，在下一个步骤 S24，CPU21 把从存储单元 28 读出的内容提供到加密和解密单元 24，它通过使用内容密钥 Kc 加密该内容。

因为存储在存储单元 28 中的内容已经由编码解码器单元 25 按照 ATRAC3 编码，所以加密和解密单元 24 对从 CPU21 接收的编码内容加密。

应当注意存储单元 28 也能够用于存储已经预先加密的内容。在这种情况下，能够消除在步骤 S24 执行的处理。

接着，在下一个步骤 S25，使用在内容服务器 3 中的 CPU21 向格式的首部加入密钥和许可 ID，加密的内容将用该格式发送。因为解密该加密数据所需要，密钥是 EKB 和 K_{EKBC}（Kc），这将在后面参照图 5 进行描述。许可 ID 被用来识别使用内容所必须的许可。接着，在下一个步骤 S26，在内容服务器 3 中使用的 CPU21 通过通信单元 29 和互联网 2 向客户机 1 发送格式化的数据。格式化的数据是格式化在步骤 S24 加密的内容和包括密钥和许可 ID 的首部的结果，密钥和许可 ID 在步骤 S25 加入到首部中。

图 5 是表示客户机 1 从内容服务器 3 接收的内容格式的图。如图中所示，格式包括首部和数据部分。

首部包括内容信息，DRM（数字权利管理）信息，许可 ID，EKB（使能密钥块）和密钥 K_{EKBC}（Kc），K_{EKBC}（Kc）是由 EKB 产生的密钥 K_{EKBC} 加密的内容密钥 Kc。应当注意到 EKB 将在后面参照图 15 进行说明。

内容信息包括内容 ID CID 和编码解码器系统的信息。内容 ID CID 是用于识别在格式的数据部分中格式化的内容的标识符。

DRM 信息包括内容的使用规则和状态。DRM 信息也包括 URL（相同资源定位器）。使用规则和状态典型地包括内容已经播放的次数和内容已经复制的次数。

URL 是一个地址，接入该地址从而获得由许可 ID 所规定的许可。更具体地说，URL 是许可服务器 4 的地址，用来在图 1 所示的内容交换系统的情况下提供需要的许可。许可 ID 是用于识别使用作为格式的数据部分被记录的内容所需要的许可的标识符。

格式的数据部分包括任意数量的加密块。每个加密块包括初始向量 IV，种

子和加密数据 Ek'c（数据），它们是对使用密钥 K'c 的内容加密的结果。

如接下来的公式所示，密钥 K'c 是通过应用内容密钥 Kc 和对散列函数的种子执行的处理的结果。种子是随机设定的值。

K'c=Hash（Kc，种子）

初始向量 IV 和种子根据加密块来改变。

内容以 8 字节单元来加密。当前阶段 8 字节通过使用在 CBC（密码块链接）模式前一阶段 8 字节加密的结果被加密。

在 CBC 模式，当内容的第一个 8 字节被加密时，8 字节的加密不在前一个阶段执行，从而不能获得前一阶段加密的结果。因此，内容的第一个 8 字节通过使用作为初始值的初始向量 IV 来加密。

因此，即使在 CBC 模式中的加密的内容加密块能够被解码，块的解码结果也可能不一定使其他加密块容易解码。

应当注意到，加密处理将在下文中参照图 46 详细描述。然而，加密系统不限于此。

如上文所述，允许客户机 1 自由地从内容服务器 3 免费获取内容。因此，大量内容本身能够被分配。

然而，当使用获取的内容时，客户机 1 需要有许可。接下来的描述参照图 6 所示的流程图说明了由客户机 1 执行的播放内容的处理。

如该图所示，流程图开始于步骤 S41，在该步骤中用户操作输入单元 26 指定想要的内容，在客户机 1 中使用的 CPU21 获取内容（CID）的标识符。标识符包括内容的标题、分配给内容的数字等。应当注意，数字指定给每个存储内容。

当内容是想要的时，CPU21 读出内容的许可 ID。为了更加明确，许可 ID 识别内容使用中要求的许可。如图 5 所示，许可 ID 包括在加密内容的首部中。

接着，在下一个步骤 S42，CPU21 形成对由步骤 S41 获得的许可 ID 表示的许可是否已经由客户机 1 获取并存储在存储单元 28 中的判断。如果由许可 ID 表示的许可还没有被客户机 1 获得，处理的流程前进到步骤 S43，在该步骤中 CPU21 执行处理以获得许可。获得许可处理的细节将在下文中参照图 7 所示的流程图来说明。

如果步骤 S42 形成的判断的输出表明由许可 ID 识别出的许可已经由客户

机 1 获得并保存在存储单元 28 中，或者如果许可能够作为步骤 S43 执行的获取许可的处理的结果而获得，处理的流程前进到步骤 S44，在该步骤中，CPU21 形成对获取的许可是否仍然在有效期限内的判断。有可能通过比较许可中规定的有效期限（这将在图 8 中说明）和当前由计时器 20 测量的日期和时间来确定获取的许可是否仍然在它的有效期限内。如果已经超过了许可的有效期限，处理的流程前进到步骤 S45，在该步骤中 CPU21 执行更新许可的处理。更新许可处理的细节将在下文中参照图 8 所示的流程图来说明。

如果步骤 S44 形成的判断的结果表明获取的许可仍然在有效期限内或者如果许可能够在步骤 S45 更新，处理的流程前进到步骤 S46，在该步骤中，CPU21 从存储单元 28 中读出加密数据并把内容存储在 RAM23 中。接着，在下一个步骤 S47，CPU21 把存储在 RAM23 中的加密内容数据以包括在图 5 所示数据部分中的加密块单元提供给加密和解密单元 24。接着，加密和解密单元 24 通过使用内容密钥 Kc 对加密内容解密。

获取内容密钥 Kc 的典型方法将在下文中参照图 15 说明。图 5 所示包括在 EKB 中的密钥 K_{EKBC} 能够通过使用图 8 中示出的设备节点密钥（DNK）获得。内容密钥 Kc 则通过使用密钥 K_{EKBC} 从数据 K_{EKBC}（Kc）中获得。

接下来，在步骤 S48 中，CPU21 将由加密解密单元 24 解密的内容提供给对该内容解码的编码解码器单元 25。接着，CPU21 通过输入/输出接口 32 把由编码解码器单元 25 解码的数据提供给输出单元 27。数据在输出到扬声器之前受到 D/A 转换。

参照图 7 所示的流程图，接下来的描述说明了在图 6 所示的流程图中的步骤 S43 执行的取得许可的处理。

客户机 1 获得预先在许可服务器 4 中分类的预先服务数据。服务数据包括叶 ID，DNK（设备节点密钥），一对适用于客户机 1 的加密和解密密钥，许可服务器 4 的解密密钥和解密密钥的证明。

叶 ID 是每个客户机 1 唯一指定的 ID。DNK（设备节点密钥）是对包括在用于许可的 EKB（使能密钥块）加密内容密钥 Kc 解密所需要的密钥，这将在下文中参照图 12 说明。

如图 7 所示，流程图开始于步骤 S61，在该步骤中 CPU21 从如图 5 所示首部中获得用于被处理许可的 ID 的 URL。如前文所述，该 URL 是一个地址，

从该地址中做读取从而获得由包括在首部中的许可 ID 确定的许可。随后，在下一个步骤 S62， CPU21 访问步骤 S61 获得的 URL。为了使它具体化，通过通信单元 29 和互联网 2 访问许可服务器 4。在那时，许可服务器 4 请求客户机 1 发送用户 ID、密码和指定将被购买的许可的许可指定信息。在使用该内容时需要该许可，该请求在图 9 中所示流程图步骤 S102 做出，这将在下文中描述。CPU21 在输出单元 27 的显示设备上显示该请求。响应于该请求，客户机 1 的用户操作输入单元 26 输入用户 ID、密码和许可指定信息。应当注意到用户在通过互联网 2 接入许可服务器 4 之前获得用户 ID 和密码。

接下来，在下一个步骤 S63 和 S64，CPU21 接收已经由用户从输入单元 26 输入的许可指定信息、用户 ID 和密码。随后，在下一个步骤 S65，CPU21 控制通信单元 29 通过互联网 2 向许可服务器 4 发送包括用户 ID、密码、许可指定信息和叶 ID 的许可请求。下文将说明叶 ID 是包括在服务数据中的信息。

如下文中所述，在图 9 所示的流程图的步骤 S109，许可服务器 4 发送基于用户 ID、密码和许可指定信息的许可。作为另一种情况，在条件不符合的情况下许可服务器 4 不发送许可，而是在图 9 所示流程图的步骤 S112 执行误差处理。

处理则前进到步骤 S66 以形成许可是否已经从许可服务器 4 接收的判断。如果许可已经被接收，处理的流程前进到步骤 S67，在该步骤中 CPU21 向存储单元 28 提供许可，并把许可存储在其中。

如果步骤 S66 形成的判断的结果表明许可没有被接收，另一方面，处理的流程前进到步骤 S68，在该步骤中，CPU21 执行误差处理。为了使它具体化，CPU21 禁止播放内容的处理，因为 CPU21 已经未能获得使用内容的许可。

如上文所述，客户机 1 能够通过获得由包括在内容中的许可 ID 表示的许可来使用内容。

应当注意到，图 7 所示流程图表示的获得许可的处理也能够在用户获得内容之前预先执行。

如图 8 所示，提供给客户机 1 的许可包括使用条件和叶 ID。

使用条件是包括在内容能够由许可所允许下载之前的截止时间、内容能够由许可所允许被复制的次数的上限或允许复制操作的最大值、结帐号、结帐的最大数量、在 CD-R 上记录的权利、内容能够复制到 PD（便携式设备）的次

数、允许使用内容的许可改为许可所有权状态（或购买的许可状态）和做使用记录的功能的信息。

参照图 9 所示的流程图，接下来的描述说明了响应于如图 7 所示的流程图表示的由客户机 1 执行的获取许可处理，由许可服务器 4 执行的向客户机 1 发送许可的处理。应当注意到，在这种情况下因为许可服务器 4 也具有包括与使用在客户机 1 中的部件相同的部件的结构，在接下来的描述中，用与图 2 中相同的附图标记来表示相同的部件。

如图中所示，流程图开始于步骤 S101，在该步骤中，使用在许可服务器 4 中的 CPU21 等待由客户机 1 做出接入。当客户机 1 接入许可服务器 4 时，处理的流程前进到步骤 S102，在该步骤中，许可服务器 4 请求客户机 1 做出接入，以发送许可指定信息（许可 ID）、用户 ID 和密码。接着，在图 7 所示的流程图的步骤 S65 中，使用在许可服务器 4 中的 CPU21 从客户机 1 通过通信单元 29 接收用户 ID、密码、叶 ID 和许可 ID，并执行读取它们的处理。

接着，在下一个步骤 S103，使用在许可服务器 4 中的 CPU21 通过通信单元 29 接入收费服务器 5，从而做出处理检验由用户 ID 和密码确定的用户的请求。当通过互联网 2 从许可服务器 4 接收这样的检验请求时，收费服务器 5 检测由用户 ID 和密码确定的用户的过去付费记载，从而确定是否有表示用户在过去没有为许可付费的记录。如果没有表示用户过去没有为许可付费的记录，收费服务器 5 发送表示许可的批准通过的检验结果。如果有表示用户在过去没有付费或其他的坏记录，收费服务器 5 则发送表示许可的批准未通过的检验结果。

接着，在下一个步骤 S104，使用在许可服务器 4 中的 CPU21 形成对于从收费服务器 5 接收的检验结果表示许可的批准通过了还是没有通过的判断。如果许可的批准通过了，处理的流程前进到步骤 S105，在该步骤中，CPU21 选择由许可指定信息指定的许可，该指定信息在步骤 S102 在存储于存储单元 28 中的许可中执行的处理中接收，并且 CPU21 从存储单元 28 中读出选择的许可。每个存储在存储单元 28 中的许可都包括含有许可 ID、形式、建立日期时间和有效期限。随后，在下一个步骤 S106，CPU21 把接收到的叶 ID 加入到许可中。而且，在下一个步骤 S107， CPU21 选择于步骤 S105 选择的许可相关联的使用条件。如果在步骤 S102 找到的使用条件已经由用户确定，若必要，把由用

户确定的使用条件加入到预先准备的使用条件中。CPU21 则把选定的使用条件加入到许可中。

随后，在下一个步骤 S108，CPU21 通过使用许可服务器 4 的密钥把标记加入许可中，以产生带有图 8 所示结构的许可。

接着，在下一个步骤 S109，使用在许可服务器 4 中的 CPU21 通过互联网 2 从通信单元 29 向客户机 1 发送带有与图 8 所示结构类似的许可。

接下来，在下一个步骤 S110，使用在许可服务器 4 中的 CPU21 通过把许可和用户 ID 和密码相关联在存储单元 28 中存储在步骤 S109 执行的处理中发送的许可，用户 ID 和密码在步骤 S102 执行的步骤中取得。如以上所述，许可包括使用条件和叶 ID。随后，在下一个步骤 S111，CPU21 执行收费程序。为了使它具体化，CPU21 请求收费服务器 5 通过通信单元 29 对由用户 ID 和密码确定的用户执行收费程序。收费服务器 5 基于用户请求执行收费处理。由许可服务器 4 执行的处理就结束了。如果用户不付由收费程序确定的费用，将来即使如上文所述请求批准许可，用户也将不能被批准该许可。

也就是说，在这样的一个用户的情况下，收费服务器 5 不通过许可的批准，作为检验是否批准许可给用户的结果。即，处理的流程从步骤 S104 前进到步骤 S112，在该步骤中，使用在许可服务器 4 中的 CPU21 执行误差处理程序。具体说来，CPU21 控制通信单元 29 输出信息通知客户机 1 读取许可不能被批准。由许可服务器 4 执行的处理就结束了。

在这种情况下，客户机 1 不能使用内容或不能对内容的加密数据解密，因为如上文所述客户机 1 未能获得许可。

图 10 是用来解释图 6 所示流程图中步骤 S 45 执行的更新许可处理的细节的流程图。步骤 S131 至步骤 S135 执行的处理基本上与图 7 所示流程图的步骤 S61 至 S65 执行的处理相同。然而在步骤 S133，CPU21 获得将被更新的许可的许可 ID，代替购买的许可的许可 ID。接着，在步骤 S1135，CPU21 将用户 ID 和密码与被更新许可的许可 ID 一起向许可服务器 4 发送。

如下文中将要描述的，响应于在步骤 S153 执行的处理中发送的信息，许可服务器 4 在图 11 所示流程图的步骤 S153 提出使用条件。接着，在下一个步骤 S136，使用在客户机 1 中的 CPU21 从许可服务器接收提出的使用条件并在输出单元 27 上显示它们。用户操作输入单元 26 以选择显示的使用条件之一和/

或新加入预定的使用条件。接着，在下一个步骤S137，CPU21向许可服务器4发送如以上描述所选择的购买使用条件或更新许可条件的申请。如下文中将描述的在图11所示流程图的步骤S154，响应于该申请，许可服务器4发送最终使用条件。接着，在下一个步骤S138，使用在客户机1中的CPU21从许可服务器4接收最终使用条件。随后，在下一个步骤S139，接收到的最终使用条件被用做已经存储在存储单元28中的许可的使用条件的更新。

图11是用来说明由许可服务器4执行的更新许可的处理以及由客户机1执行的请求更新许可的操作的处理的流程图。

如图中所示，流程图开始于步骤S151，在该步骤中许可服务器4由客户机1接入。接着，在下一个步骤S152，使用在许可服务器4中的CPU21从客户机1中接收更新许可请求以及在步骤S135由客户机1接收的许可指定信息。

随后，在下一个步骤S153，CPU21按照更新许可的请求读出将被更新的许可的使用条件，或从存储单元28读出更新许可的条件。CPU21则向客户机1发送该条件。

响应于发送的条件，假定在图10所示流程图的步骤S137执行的处理中客户机1的用户输入购买使用条件的申请。在这种情况下，在下一个步骤S154，使用在许可服务器4中的CPU21产生的被采用的使用条件的数据并向客户机1发送数据。如上所述，客户机1使用接收到的使用条件作为对许可的已经分类的使用条件的更新。如上文所述，使用条件在步骤S139执行的处理中被更新。

在本发明中，设备的密钥和许可的密钥基于图12所示的广播加密系统的原理来管理。密钥组成分层的树结构。在分级的层底部的每个叶都对应于每个设备的密钥。在图12所示的典型结构中，产生对应于16个设备或16个许可的16个密钥0到15。

每个用圆环标记表示的密钥放置在树结构的节点上。根密钥KR放置在树结构顶部上的根接点。在第二分级层节点上有密钥K0和K1。在第三分级层节点上，放置有密钥K00到K11。在第四分级层上的节点上，有密钥K000至K111。在分级层底部节点上的叶或设备节点是密钥K0000到K1111。

在分级树结构中，例如密钥K0010和K0011每个都是密钥K001的次级。在相同的方式中，密钥K000和K001每个都是密钥K00的次级。用相同的标记，在更高的分级层上，密钥K00和K01每个都是密钥K0的次级。同样，密

钥 K0 和 K1 每个都是根密钥 KR 的次级。

使用内容要求的密钥包括分级层底部的设备节点上的叶和包含根密钥 KR 的更高分级层节点上的密钥。包括根密钥 KR 的更高分级层上的叶和密钥形成通路。例如，使用内容 3 所要求的密钥由包括密钥 K0011、K001、K00、K0 和 KR 的每个密钥来管理，在对应于叶 ID 的许可的基础上它们形成开始于叶 K0011，结束于根密钥 KR 的通路。

本发明提供的内容交换系统典型地采用图 12 所示的管理设备密钥和位于节点上的许可的原理，节点形成图 13 所示的 8+24+32 层结构。在图 13 所示的结构中，在根节点以下有 8 个附属的分级层。8 个分级层的每个节点上的密钥与分类相关联。分类的例子是使用半导体存储器比如记忆棒的设备的分类和用于接收数字广播的设备的分类。

分类节点之一是由本发明提供的用于管理许可的叫做 T 系统的系统的根节点。

详细地说，T 系统的根节点的次级是 24 分级层上的节点。每个次级节点的密钥与许可相关联。因此，有可能规定 2^{24} 个许可或大约 1.6 千万或大约 160 万个许可。而且在更低层上的次级是 32 分级层，这允许规定 2^{32} 个用户（或客户机 1）或大约 40 亿或大约 40 亿用户（或客户机 1）。位于 32 分级层节点上的密钥每个都是 DNK（设备节点密钥）。

用于设备的密钥或用于许可的密钥沿着穿过 64（=8+24+32）分级层的节点的通路放置。从而，这样的路径与设备或许可相关联。具体地说，用于加密内容的内容密钥由位于通过与内容许可相关联的路径的节点上的密钥来加密。在上一分级层的密钥通过使用直接在分级层下一层的它的直接次级密钥来加密并放入 EKB，这将在下文中参照图 15 描述。根分级层上的 DNK 不放入 EKB，但包括在将被批准给用户的客户机 1 的服务数据中。客户机 1 使用包括在解密密钥的许可中的 DNK，该密钥位于恰在 DNK 上的分级层上并包括在图 15 所示的 EKB 中。EKB 与内容的数据一起分配。客户机 1 则使用解密密钥对密钥解密，该密钥位于解密密钥正好上一个分级层上并包括在 EKB 中。该解密程序被重复执行直到客户机 1 能够获得所有位于通过与许可相关联的路径的节点上的密钥。

图 14 是表示典型的分类分类，每个分类与分级树结构的密钥相关联。如

图 14 所示，在分级树结构顶部，设置根密钥 KR2301。在根密钥 KR2301 下面的中间分级层上，设置节点密钥 2302。在分级层的底部，设置叶密钥 2303。每个设备有叶密钥、节点密钥和根密钥。设备所有的节点密钥沿着路径提供，该路径与设备相关联并连接叶密钥与根密钥。

在从根密钥开始的第 M 分级层上的预定节点被设为分类节点 2304。在图 13 所示的例子中，设 M 是 8。第 M 分级层上的每个节点被用做为适合指定分类的设备设定根密钥的节点。也就是说，分类的设备与开始于第 M 分级层上的节点、穿过第（M+1）和更低分级层并结束于根部分级层的叶上的路径相关联。

假定，记忆棒（商标）的分类设在图 14 所示的分级树结构中第 M 分级层上的节点 2305。在这种情况下，低于该节点 2305 的连接的节点和叶被用作特别为包括各种使用记忆棒的设备的分类而提供的节点和叶。即，低于节点 2305 的节点和叶被定义为一组节点和一个叶，该组节点和叶与记忆棒的分类中定义的装置相关。

另外，低于第 M 分级层几级的分级层上的节点可以被设为子分类节点 2306。在图 14 所示的分级树结构中，低于提供有节点 2305 的记忆棒分类分级层两级的分级层上的节点被设为子分类节点，也就是用作包括在设备的分类中的子分类的节点，其中每个设备都使用记忆棒。而且，在低于 2306 作为只播放设备的子分类的分级层上设置用于具有播放音乐功能的电话的节点。这样的电话包括在只播放设备的分类中。而且，在节点 2307 下面的分级层上提供有 PHS 节点 2308 和蜂窝电话节点 2309。PHS 和蜂窝电话包括在具有播放音乐功能的电话分类中。

此外，分类子分类不仅提供给设备也提供给由生产商、内容提供者和独立单元或任意数量单元的收费机构控制的节点，它们可以是处理单元、控制单元、显示服务单元等。这些部件每个都指通用技术术语所说的一个实物。假定分类节点被设为特别提供给游戏机制造商销售的游戏机 XYZ 的根节点。在这种情况下，游戏机制造商能够通过在游戏机 XYZ 中存储节点密钥和叶密钥销售游戏机 XYZ，节点密钥和叶密钥提供在低于根节点的分级层上。接着，分配加密内容或各种密钥，或者通过产生 EKB 更新密钥。EKB 包括节点密钥和叶密钥，它们提供在低于根节点的分级层上。以这种方式，有可能分配只能被根节点下的设备使用的数据。

如上所述，一个节点被用作根节点并且低于根节点的分级层上的节点每个都设为分类相关节点或子分类相关节点。用这种方式，比如制造商或内容提供商的机构能够用在根节点上用它本身作为根密钥的密钥产生 EKB（使能密钥块）并向适合于低于根节点的分级层的设备分配 EKB，该机构管理分类分级层或子分类分级层上的根节点。因此，有可能在完全不影响适合于不作为根节点次级分类节点的设备的情况下，更新 EKB 的密钥。

假定在图 12 所示的树结构中，属于一组的四个设备 0、1、2 和 3 共享通用密钥 K00、K0 和 KR 作为节点密钥。通过使用该节点-密钥-共享结构，通用内容密钥可以只提供给设备 0，1，2 和 3。例如，由设备 0，1，2 和 3 共享的节点密钥 K00 本身被设为公用内容密钥。以这种方式，有可能不用发送新密钥而设置设备 0、1、2 和 3 公用的内容密钥。或者，新内容密钥 Kcon 通过使用节点密钥 K00 被加密，产生加密值 Enc（K00，Kcon），该加密值再通过网络分配给设备 0，1，2 和 3 或通过在存储介质中保存值 Enc（K00，Kcon）分配给设备 0、1、2 和 3。用这种方式，只有设备 0、1、2 和 3 能够通过使用设备 0、1、2 和 3 共享的公用节点密钥 K00 解密该数值 Enc（K00，Kcon）以产生内容密钥 Kcon。应该注意到符号 Enc（Ka，Kb）表示作为通过使用密钥 Ka 加密密钥 Kb 的结果获得的数据。

此外，假定在点时刻 t 发现设备 3 所有的密钥 K0011、K001、K00、K0 和 KR 已经被黑客分析并识别。在这种情况下，为了保护此后在系统（或一组设备 0、1、2 和 3）中交换的数据，设备 3 需要从系统中分离出来。另外，节点密钥 K001、K00、K0 和 KR 需要分别被更新为新密钥 K（t）001、K（t）00、K（t）0 和 K（t）R 发送到设备 0、1 和 2。应当注意到，符号 K（t）aaa 是一个时间点 t 产生的更新密钥并通过更新密钥 Kaaa 获得。

分配更新后的密钥的处理在下文中说明。例如，密钥按照如下方式更新。在如上文所述处理为设备 0、1 和 2 更新密钥的情况下，一个表通过网络供给设备 0、1 和 2，或通过在存储单元中保存该表并向设备 0、1 和 2 提供存储单元把表提供给设备 0、1 和 2。该表是如图 15A 所示叫做 EKB（使能密钥块）的块数据。应当注意到 EKB（使能密钥块）包括加密密钥，它用于向与类似图 12 所示的树结构的根部分级层节点的叶相关联的设备分配重新更新后的密钥。EKB（使能密钥块）也叫做 KRB（密钥更新块）。

图 15A 所示 EKB（使能密钥块）被构造为块数据，该块数据只能由将被更新的节点密钥所要求的设备更新。图 15A 所示的典型的 EKB 是以向图 12 所示的树结构的设备 0、1 和 2 分配时间点 t 产生的更新的节点密钥为目的而建立的块数据。由图 12 明显看出，设备 0 和 1 每个都需要 K（t）00、K（t）0 和 K（t）R 作为更新的节点密钥。另一方面，设备 2 需要 K（t）001、K（t）00、K（t）0 和 K（t）R 作为更新的节点密钥。

如图 15A 所示，EKB 包括多个加密密钥。从图 15A 所示表格的顶部开始第五栏的加密密钥是 Enc（K0010，K（t）001），这是通过使用设备 2 所拥有的叶密钥 K0010 加密的更新后的节点密钥 K（t）001。从而设备 2 能够通过对使用设备 2 本身拥有的叶密钥 K0010 的加密密钥 Enc（K0010，K（t）001）解密，获得更新的节点密钥 K（t）001。另外，通过使用作为解密结果的获得的更新后的节点密钥 K（t）001，有可能对图 15A 所示表格中的第四栏加密密钥 Enc（K（t）001，K（t）00）解密以产生更新后的节点密钥 K（t）00。

因此，在这样的连续解密过程中，图 15A 所示表格的第二栏的加密密钥 Enc（K（t）00，K（t）0）被解密，产生更新后的节点密钥 K（t）0，它再被用于对第一栏的加密密钥 Enc（K（t）0，K（t）R）解密以产生更新的节点密钥 K（t）R。

另一方面，节点密钥 K000 不是将被更新的密钥。与节点 0 和 1 相关联的设备 0 和 1 所需要的更新的节点密钥分别是 K（t）00、K（t）0 和 K（t）R。分别与节点 0 和 1 相关联的设备 0 和 1 每个都使用设备密钥 K0000 和 K0001 对图 15A 所示表格的第三栏的加密密钥 Enc（K000，K（t）00）解密以获得更新后的节点密钥 K（t）00。因此，在连续的解密过程中，图 15A 所示的表格中第二栏的加密密钥 Enc（K（t）00，K（t）0）被解密，产生更新后的节点密钥 K（t）0，它再被用于对第一栏的加密密钥 Enc（K（t）0，K（t）R）解密，产生更新后的节点密钥 K（t）R。用这种方式，设备 0、1 和 2 每个都能够获得更新后的节点密钥 K（t）R。

应当注意到，图 15A 所示的索引是节点密钥和叶密钥的绝对地址。每个节点密钥和叶密钥都被用作对图的右侧加密密钥解密的解密密钥。

当没有必要更新图 12 所示树结构的上部分级层上的节点密钥 K（t）0 和根密钥 K（t）R，同时有必要执行只更新节点密钥 K00 的处理时，更新后的密

钥K（t）00能够通过使用图15B所示的EKB（使能密钥块）分配给设备0、1和2。

图15B所示的EKB能够被用于向属于指定组的设备分配典型的共用新内容密钥。假定由图12中虚线围起来的属于同一组的设备0、1、2和3每个都使用记录介质并需要新的公用内容密钥K（t）con。在这种情况下，数据Enc（K（t）00，K（t）con）和图15B所示的EKB一起分配给设备0、1、2和3。数据Enc（K（t）00，K（t）con）是设备0、1、2和3公用的新的更新内容密钥K（t）con加密的结果。新的更新内容密钥K（t）con通过使用K（t）00来加密，K（t）00是设备0、1、2和3公用节点密钥K00加密的结果。通过这种处理，加密的数据Enc（K（t）00，K（t）con）可以被分配，从而其他组的设备比如设备4不能对加密的数据解密。

也就是说，设备0、1和2每个都能够通过使用密钥K（t）00对加密的数据解密，从而获得时间点t的产生的内容密钥K（t）con，其中K（t）00作为EKB处理的结果而获得。

图16是表示由设备0执行的获得时刻t产生的内容密钥K（t）con的典型处理的图，该设备已经通过记录介质接收数据Enc（K（t）00，K（t）con）和图15B所示的EKB。如上文所述，数据Enc（K（t）00，K（t）con）是对设备0、1、2和3公用的重新更新的内容密钥K（t）con加密的结果。即，在该典型处理中，通过使用EKB分配的加密信息数据是内容密钥K（t）con。

如图16所示，在与以上描述相同的EKB处理中，设备0通过使用时间点t产生的EKB和自己预先存储在记录介质中的节点密钥K000产生节点密钥K(t)00。EKB已经存储在记录介质中。接着，设备0使用作为解密结果而得到的更新的节点密钥K（t）00，从而解密更新的内容密钥K（t）con。为了随后的使用，设备0则通过使用只由设备0所有的叶密钥K0000对该密钥加密。

图17是表示EKB（使能密钥块）的典型格式的图。模型601是表示EKB（使能密钥块）模型的标识。应当注意到模型601有确定最新的EKB和表示与内容之间的关系的功能。深度是用作EKB（使能密钥块）接收站的装置的分级树结构中分级层的数。数据指示器603是指示EKB（使能密钥块）在数据部分606中位置的指示器。标记指示器604是指示标记607位置的指示器，签名指示器605是指示签名608位置的指示器。

数据部分 606 是典型的加密的更新节点密钥，即作为图 16 所示的更新的节点密钥加密的结果而获得的加密密钥。

标记 607 是表示加密的节点密钥和加密的叶密钥之间位置关系的标记。加密的节点密钥和加密的叶密钥包括在数据部分 606。提供标记的规则参照图 18 来说明。

图 18 是表示发送前面参照图 15A 说明的 EKB（使能密钥块）的例子的图。在这种情况下，数据如图 18B 所示。在那一时刻包含在加密密钥中的顶节点的地址被指定为顶节点地址。在该例子中，因为包括更新后的根密钥 K（t）R，所以顶结点密钥是 KR。在这种情况下，例如第一栏的数据 Enc（K（t）0，K（t）R）对应于图 18A 所示的分级树结构中的位置 P0。第二栏的数据 Enc（K（t）00，K（t）0）对应分级树结构中位置 P0 的左下方上的位置 P00。如果在低于分级树结构的预定位置的分级层上有数据，则标记设为 0。如果在低于分级树结构的预定位置的分级层上没有数据，则标记设为 1。标记按照下文中描述的如下格式设定：{左（L）标记，右（R）标记}。在对应于图 18B 所示的第一栏的数据 Enc（K（t）0，K（t）R）的位置 P0 的左下方的位置 P00 上有数据。因此，L 标记设为 0。另一方面，在位置 P0 的右下方位置上没有数据。在这种情况下，R 标记设为 1。以这种方式，为每个数据设置标记。图 18C 是表示包括典型的数据片阵列和标记阵列的结构的图。

标记被设置用来表示对应数据 Enc（Kxxx，Kyyy）位于树结构中哪个位置。保存在数据部分 606 中的密钥数据 Enc（Kxxx，Kyyy）等只是用简单的方式加密的密钥的阵列。然而用以上描述的标记，有可能识别作为数据存储的加密密钥在树结构中的位置。没有以上描述的标记，如用先前参照图 15 说明的结构的情况一样，也有可能通过使用与加密数据片相关联的节点索引构造数据。以下给出了数据结构的一个例子：

0：Enc（K（t）0，K（t）R）

00：Enc（K（t）00，K（t）0）

000：Enc（K（t）000，K（t）00）

然而在使用这样的索引的结构中，产生了冗余数据，从而数据量增加了。结果，这样的结构不希望用于通过网络分配或用于其他目的。然而通过使用作为表示密钥位置的索引数据的标记，密钥的位置能够只通过使用少量数据来识

别。

EKB 格式进一步通过再次参照图 17 来说明。签名 608 是由发出 EKB（使能密钥块）的机构放置的一个电子签名。这样的机构的例子是密钥管理中心（许可服务器 4），内容提供商（内容服务器 3）和收费机构（收费服务器 5）。接收 EKB 的设备确认 EKB 是通过信号验证由授权的 EKB 发行人发出的有效的 EKB。

有可能基于由如上所述的许可服务器 4 发出的许可，利用由内容服务器 3 提供的内容把处理过程总结为图 19 所示的形式。

如图所示，当内容服务器 3 向客户机 1 提供内容时，许可服务器 4 向客户机 1 发出许可。内容是 Enc（Kc，内容），这是表示内容已经被内容密钥 Kc 加密的符号。内容密钥 Kc 通过使用根密钥 KR 来加密以产生 Enc（KR，Kc）。根密钥 KR 从 EKB 获得并对应于图 5 所示的密钥 K_{EKBC}。内容密钥 Enc（KR，Kc）和 EKB 随后被附加到加密内容中。内容密钥 Enc（KR，Kc）、EKB 和加密内容最终提供给客户机 1。

如图 20 所示，图 19 所示实施例中的 EKB 典型地包括 Enc（DNK，KR），这是表示根密钥 KR 已经由 DNK 加密的符号。因此，通过使用包括在服务数据中的 DNK，客户机 1 能够从 EKB 获得根密钥 KR。接着，有可能通过使用根密钥 KR 解密 Enc（KR，Kc）的获得内容密钥 Kc。最终，有可能通过使用内容密钥 Kc 解密 Enc（KR，内容）获得内容。

通过以这种方式将 DNK 指定给每个客户机 1，也有可能按照图 12 和 15 所示的原则单独地撤销客户机 1。

另外，通过包括作为分配中的数据部分的另外的许可叶 ID，服务数据与许可相关联，从而有可能避免客户机 1 中的非法复制操作。

而且，通过对每个客户机分配作为服务数据的密钥和证明，有可能建立这样的内容，即用于客户机 1 使用的该内容的密钥和证明被用于防止最终用户执行复制内容的非法操作。

密钥和证明的使用将在下文中参照图 28 的流程图来说明。

如前面参照图 13 所描述的，按照本发明，用于管理分类节点上的许可的 T 系统与用于使用内容的每个设备的分类相关。因此，多个 DNK 能够由相同设备所拥有。结果，属于不同分类的内容能够用一个设备管理。

02.03.12

图 21 是表示对一个设备分配多个内容的的示意性的图。更明确地说，用于使用客户机 1 的许可记录在基于 T 系统的设备 D1 上，DNK1 分配给内容 1。通过相同的方式，分配了 DNK2 的内容 2 可以通过从 CD 向记忆棒传送内容 2 记录在设备 D1 中。以这种方式，设备 D1 能够同时传递两个内容，即内容 1 和内容 2，这两个内容由不同的系统即 T 系统和设备管理系统来分配。该特征不能在只向设备分配一个 DNK 的情况下实现。这种情况的一个例子是当新的 DNK 被分配时已经分配的 DNK 被删除的情况。

另外，例如，图 22 所示的许可分类 1 和 2 被分配给图 13 所示的 32 下面的分级层的每一个三角形。通过这样的分配，分类被划分为子分类用来管理更小的组，比如内容的类型、内容的等级、内容的零售商店和内容的分配服务。

在图 22 所示的典型的分配中，例如，许可 1 和 2 分别属于爵士类型和摇滚类型。许可分类 1 与内容 1 和 2 相关联，内容 1 和 2 每个都具有 1 的许可 ID 并分配给用户 1 和 3。许可分类 2 包括内容 3、4 和 5，内容 3、4 和 5 每个均具有 2 的许可 ID 并分配给用户 1 和 3。

如上所述，按照本发明，能够对每个分类执行独立的密钥管理。

另外，取代在设备和/或介质中嵌入 DNK，DNK 也能够在由许可服务器 4 执行的分类处理中下载到每个设备和/或每个介质，从而实现允许用户购买该密钥的系统。

提供一种不考虑采用的是何种技术，建立内容后通过采用使用内容的任何技术，都能够在所有申请中使用的内容是理想的。例如，希望提供一种能够用在具有不同内容分配服务或不同使用条件的领域中的内容。为了提供这样的内容，按照本发明，如上文所述，具有鉴别站功能的许可服务器 4 向用户（客户机 1）分配密钥和用于密钥的公开的密钥的证明。接着，每个用户使用密钥建立将放置在内容中的印记，以便确保内容的完整并从而防止内容被伪造。

以上描述的情况的典型处理参照图 23 所示的流程图来说明。更明确地说，处理是由用户执行的从存储单元 28 中的 CD 播放记录数据的窃取过程。

如图中所示，流程图开始于步骤 S171，在该步骤中，是用在客户机 1 中的 CPU21 接收输入的来自通信单元 29 从 CD 播放的记录数据。随后，在下一个步骤 S172，CPU21 形成对在步骤 S171 输入的记录数据是否包括嵌在内容数据中的水印的判断。水印包括 3 比特 CCI（复制控制信息）和 1 比特触发器。如

果检测到水印，处理的流程走到步骤 S173，在该步骤中 CPU21 执行提取水印的程序。如果没有检测到水印，则跳过水印提取程序。

随后，在步骤 S174，CPU21 产生将为内容所记录的首部数据。首部数据包括内容 ID、许可 ID、表示用于获得许可和水印的访问目标的 URL。

接下来，在下一个步骤 S175，通过使用 CPU21 本身的密钥，CPU21 产生基于首部数据的数字签名，该首部数据在步骤 S174 执行的处理中产生。密钥已经在图 7 所示的流程图的步骤 S67 从许可服务器 4 中获得。

接着，在下一个步骤 S176，CPU21 控制加密和解密单元 24 通过使用内容密钥加密内容。内容密钥已经在得到内容的同一时刻得到（见图 5 或 9）。

接下来，在下一个步骤 S177，CPU21 用文件格式在磁光盘 43 上记录数据。有代表性的磁光盘 43 是迷你盘。

应当注意到，在迷你盘用作记录介质的情况下， CPU21 在步骤 S176 向编码解码器单元 25 提供内容。编码解码器单元 25 按照典型的 ATRAC3 系统编码内容。编码的内容还由加密和解密单元 24 进一步加密。

图 24 是表示在记录介质上记录的内容的模式。从加密内容（E（At3））提取的水印 WM 记录在内容外的首部中。

图 25 是表示内容记录在记录介质中所用文件格式的详细结构的图。从该典型结构看出，记录了包括内容 ID（CID）、许可 ID（LID）、URL 和水印（WM）的首部。另外，记录了 EKB、数据 Enc（KR，Kc）、证明（Cert）、数字首部（Sig（Header）），数据 Enc（Kc，内容），元数据和标记。数据 Enc（Kr，Kc）是使用根密钥 KR 加密内容密钥 Kc 的结果，其中数据 Enc（Kc，内容）是使用内容密钥 Kc 加密内容的结果。数字首部 Sig（Header）已经在首部的基础上产生。

水印嵌入在内容中。如图 24 和 25 所示，除了加到内容的中间之外，水印也放在首部中从而作为水印的内容中嵌入信息能够快速并简单地被检测。因此，有可能快速形成内容是否能够被复制的判断。

应当注意元数据典型地表示唱片封套、图片、歌词和其他信息。标记将在下文中参照图 31 进行描述。

图 26 表示用作披露的密钥的证明的典型的披露的密钥证明的图。通常披露的密钥证明是由披露的密钥加密系统中的 CA（证明授权方）发出的证明。

披露的密钥证明由授权方通过向提供给证明授权方的披露密钥和用户 ID 中加入比如有效期限这类的信息以及在其中放入证明授权的数字签名而产生。按照本发明，许可服务器 4 或内容服务器 3 发出证明和密钥，也发出披露的密钥。因此，通过向许可服务器 4 提出比如用户 ID 和密码的信息并在其中分类，用户能够获得披露的密钥证明。

在图 26 中示出的披露的密钥证明包括一个消息。该消息包括证明的版本号、由许可服务器 4 向证明的用户发出的序列号、用于数字签名的运算法则和参数、证明授权方的名称、证明的有效期限、分配给证明的用户的 ID 和证明用户的披露的密钥。在这种情况下，证明授权方是许可服务器 4。分配给用户的 ID 是节点 ID 或叶 ID。由用作证明授权方的许可服务器 4 产生的数字签名被附加到该消息中。数字签名是通过使用许可服务器 4 的密钥基于由消息的混乱信息函数的应用产生的混乱信息值建立的数据。

在图 12 所示的典型密钥组织的情况下，例如，节点 ID 或叶 ID 对设备 0 是‘0000’，对设备 1 是‘0001’以及对设备 15 是‘1111’。在这样的 ID 的基础上，从而有可能确定由 ID 确定的设备（机构）位于树结构中的哪个位置，即树结构中的哪个叶或哪个节点。

通过以这种方式与内容分离地分配使用内容所要求的许可，内容能够以更高的自由度分配。采用任意方法获得的内容和通过任意路线获得的内容能够因此被统一地传递。

另外，通过构建图 25 所示的文件格式，当内容通过互联网分配甚至当内容提供给 SDMI（安全的数字音乐发端）设备时，无须置疑，带有这样的格式的内容的复制权可以被管理。

而且，即使内容通过在记录介质上记录内容来提供或通过图 27 所示的互联网 2 来提供，例如通过执行相同的处理，对典型的用作 SDMI（安全的数字音乐发端）设备的预定 PD（便携式设备）来说有可能检验出内容。

通过参照图 28 所示的流程图，接下来的描述说明了为与客户机 1 不同的客户机如 PD 检验出内容的处理。

如图中所示，流程图开始于步骤 S191，在该步骤中，CPU21 形成对数字签名是否已经放入到内容中的判断。如果判断的结果表明数字签名已经放入内容中，处理的流程前进到步骤 S192，在该步骤中 CPU21 提取披露的密钥证明

并通过使用作为证明授权方的许可服务器 4 的披露的密钥执行鉴别证明的处理。详细说来，客户机 1 从许可服务器 4 获取用于许可服务器 4 的密钥的披露的密钥，并使用该披露的密钥对放入披露的密钥证明中的数字签名解密。如前文中参照图 26 所描述的，数字签名是基于用作证明授权方的许可服务器 4 的密钥产生的并能够通过使用许可服务器 4 的揭露的密钥解密。而且，CPU21 对证明的全部消息应用散列函数以产生混乱信号值。接着，CPU21 比较产生的混乱信号值和解密数字签名获得的混乱信号值。如果产生的混乱信号值与解密数字签名获得的混乱信号值相匹配，确定消息不是错误消息。如果产生的混乱信号值与解密数字签名获得的混乱信号值不匹配，则该证明被确定是错误证明。

从而，在下一个步骤 S193，CPU21 形成对证明是否已经被伪造的判断。如果判断结果表明该证明没有被伪造，处理的流程前进到步骤 S194，在该步骤中 CPU21 执行通过使用 EKB 鉴别该证明。通过检验 EKB 是否能够根据包含在证明中的叶 ID 被描绘，鉴别该证明。对于叶 ID 上的更多信息参照图 26。鉴别参照图 29 和 30 在下文中进行说明。

如图 29 所示，假定拥有叶密钥 K1001 的设备是已经取消的设备。在这种情况下，如图 30 所示的具有标记和数据（加密的密钥）的 EKB 被分配给设备，每个设备对应一个叶。为了取消图 29 所示的设备‘1001’，该 EKB 是用于更新密钥 KR、K1、K10 和 K100 的 EKB。

除了对应取消的设备‘1001’的叶之外的所有叶都能够获得更新的根密钥 K（t）R。也就是说，因为在分级层上低于节点密钥 K0 的任意叶在设备中都有未更新的节点密钥 K0，所以叶能够通过对用密钥 K0 加密的密钥 Enc（K0，K（t）R）解密获得更新后的根密钥 K（t）R。

另外，在节点密钥 K11 下面的分级层上的叶能够通过使用未更新的节点密钥 K11 解密 Enc（K11，K（t）1）获得更新后的节点密钥 K（t）1。此外，可以通过使用更新节点密钥 K（t）1 解密 Enc（K（t）1，K（t）R）来获得更新后的根密钥 K（t）R。通过相同的方式，在节点密钥 K101 下面的分级层上的叶也能够获得更新后的根密钥 K（t）R。

另外，拥有未取消的叶密钥 K1000 的设备‘1000’能够通过对使用它自己的叶密钥 K1000 解密的 Enc（K1000，K（t）100）获得节点密钥 K（t）100。接着，设备使用节点密钥 K（t）100 一个密钥接一个密钥地解密分级层上一层

的节点密钥，最终获得更新后的根密钥K（t）R。

另一方面，因为取消的设备‘1001’不能通过在它自己叶上方上一个分级层上的执行EKB处理获得更新后的节点密钥K（t）100，该设备因此不能够最终获得更新后的根密钥K（t）R。

一个被授权的设备即没有被取消的客户机1从许可服务器4接收带有图30所示的标记和数据的EKB并在设备中存储它们。

从而，每个客户机能够通过使用标记执行EKB追踪程序。EKB追踪程序是形成密钥分配树是否能够从顶端的根密钥找出的判断的程序。

假定图29所示分配给叶‘1001’的‘1001’的叶ID有4比特，即‘1’、‘0’、‘0、’和‘1’。EKB追踪程序被执行以形成树是否能够通过从第一比特开始向下一个比特接一个比特检验直到最后一个信号比特被追踪的判断。准确地说，‘1’比特表示追踪应当向右侧进行，而‘0’比特表示追踪应当向左侧进行。

因为ID‘1001’中最高有效位是‘1’，追踪应当从图29所示的根密钥KR向右侧进行。EKB的第一标记，即具有数字0的标记是0：{0，0}，这表示数据在两个分支中都存在。在这种情况下，因为追踪能够继续向右侧进行，所以有可能达到节点密钥K1。

接着，追踪继续向低于节点密钥K1的分级层上的节点进行。因为ID‘1001’的第二个比特是‘0’，所以追踪向左侧继续。带有数字1的标记表明数据是否存在于低于节点密钥K0的分级层左侧。表示数据是否存在于低于节点密钥K1的分级层上的标记是具有数字2的标记。如图30所示，带有数字2的标记是2：{0，0}，这表示数据在两个分支上都存在。因此，追踪继续向左侧进行并能够达到节点密钥K10。

而且，因为ID‘1001’的第三比特是0，追踪继续向左侧进行。在那一时刻，表示数据是否存在于低于节点密钥K10的分级层上的数据是具有数字3的标记。具有数字3的标记是3：{0，0}，它表示数据在两个分支上都存在。因此，追踪继续向左侧进行并能够达到节点密钥K100。

而且，因为ID‘1001’的最低有效位是1，追踪继续向右侧进行。具有数字4的标记对应于节点密钥K11。表示数据是否存在于低于节点密钥K100的分级层上的数据是具有数字5的标记。具有数字5的标记是5：{0，1}，它表

示在右侧不存在数据。结果，因为不能达到节点‘1001’，具有 ID ‘1001’的设备被确定为不能通过使用 EKB 获得更新后的根密钥的设备，即被取消的设备。

另一方面，例如具有叶密钥 K1000 的设备 ID 是‘1000’。因此，当以 EKB 中的标记为基础的 EKB 追踪处理按上述方式进行时，有可能达到节点‘1000’。结果，具有 ID‘1000’的设备被确认为授权的设备。

再回来参照图 28。在下一个步骤 S195，CPU21 形成证明是否已经在步骤 S194 执行的鉴别处理的结果基础上被取消的判断。如果证明还没有被取消，处理的流程前进到步骤 S196，在该步骤中执行通过使用包含在证明中的披露的密钥鉴别数字签名的处理。

即，如图 26 所示，该证明包括证明用户（或内容作者）的披露的密钥。披露的密钥被用来鉴别图 25 所示的数字签名 Sig（Header）。详细地说，披露的密钥被用来解密数字签名 Sig（Header）以产生混乱信号值。该混乱信号值与通过对如图 25 所示的首部应用散列函数所获得的混乱信号值相比较。如果两个混乱信号值互相匹配，则首部被确认为未经伪造的首部。否则，首部被确定为已经被伪造。

随后，在下一个步骤 S197，CPU21 形成首部是否已经被伪造的判断。如果首部没有被伪造，处理的流程前进到步骤 S198，在该步骤中鉴别水印。接着，在下一个步骤 S199，CPU21 形成水印鉴别结果是否表示有可能检验的判断。如果有可能检验，处理的流程前进到步骤 S200，在该步骤中 CPU21 执行检验。具体地说，CPU21 把内容传送到客户机 1，客户机 1 作为检验的目的地并在其中进行复制。

如果步骤 S191 形成的判断的结果表示数字签名不存在，在步骤 S193 形成的判断的结果表示证明已经被伪造，在步骤 S195 形成的判断的结果表示证明不能通过使用 EKB 被鉴别，步骤 S197 形成的判断的结果表示数字签名鉴别的结果表明首部已经被伪造或者在步骤 S199 形成的判断的结果表示水印包括禁止检验的说明，则处理的流程前进到步骤 S201，在该步骤中，执行错误处理程序，也就是说，在这种情况下，禁止检验。

如上所述，证明和密钥从许可服务器 4 分配给用户。通过在内容建立时加入数字签名，能够确保内容作者的真实性。结果，能够避免内容的非法传播。

另外，通过在内容建立时检测水印并向数字签名中加入水印，能够避免水印的伪造。从而能够确保内容的真实性。

结果，内容一旦建立，就不用考虑内容以何种格式分配就能确保原始内容的真实性。

另外，内容没有使用条件。代替它的是将使用条件加入到对内容的许可中。从而，通过改变包含在许可中的使用条件，也能够修改使用内容的条件。

接下来，说明使用标志的方法。如上文所述按照本发明，使用条件不加入到内容中，而加入到对内容的许可中。但是，使用情况可能随着一个个内容而改变。为了解决该问题，如图 25 所示按照本发明将标志加入到内容中。

因为许可与多个内容相关，所以只用包含在许可中的使用条件来描述每个内容的使用情况是困难的。为了解决该问题，通过向内容中加入使用情况，有可能在管理许可的同时管理各个内容。

如图 31 所示，标志典型地包括分配给用户的 ID（叶 ID）、所有权标记、使用开始时间和复制数量。

另外，标志也包括附加的数字签名，它是在比如叶 ID、所有权标记、使用开始时间和复制数量这些信息基础上建立的。

例如，当用户买允许内容只在预定时间段内被使用的许可时，或当使用期限改变为永久使用期限时加入所有者标记。当内容的使用在预定时间段内开始时，确定使用开始时间。假定下载内容的时间段被限制。在这种情况下，如果内容在限定的时间段内下载，内容实际上下载的日期和时间作为使用开始时间被记录。在这种情况下，证实在时间段内内容的合法使用。

复制数量是作为记录而记载的执行复制内容操作的次数。

参照图 32 所示的流程图，接下来的描述说明了当用户购买许可时执行的向内容中加入标志的处理。

如图中所示，流程开始于步骤 S221，在该步骤中 CPU21 按照由用户经输入单元 26 输入的命令通过互联网 2 接入许可服务器。

接着，在下一个步骤 S222，CPU21 获取由用户通过输入单元 26 键入的输入并按照输入向许可服务器 4 发送购买许可的请求。

响应于该请求，许可服务器 4 在图 33 所示的流程图中的步骤 S242 提出购买许可的价格，这在下文中将参照图 33 的流程图进行说明。随后，在下一个

步骤 S223，用在客户机 1 中的 CPU21 接收由服务器 4 发出的价格并在输出单元 27 上显示该价格。

在显示的价格的基础上，用户形成是否同意该价格的判断。用户向输入单元 26 输入判断的结果。

接着，在下一个步骤 S224，在输入到输入单元 26 中的判断结果的基础上，CPU21 形成价格是否已经被同意的判断。如果价格已经被同意，处理的流程前进到步骤 S225，在该步骤中 CPU21 执行通知许可服务器 4 价格已经被同意。

接收到该通知，许可服务器 4 发出表示以该价格购买许可的信息，即包括图 33 所示流程图中在步骤 S244 描述的所有权标记的标志。随后，在下一个步骤 S226，用在客户机 1 中的 CPU21 接收许可服务器 4 发出的标志。接着，在下一个步骤 S227，CPU21 执行把标志嵌入到内容中的处理。从而包括图 31 所示的描述的所有权标记的标志记录在与购买的许可相关的内容中作为内容的标志。另外，因为在那一时刻消息被更新，CPU21 也更新图 25 所示的数字签名并在记录介质中存储更新后的数字签名。

如果在步骤 S224 形成的判断的结果表明由许可服务器 4 提出的价格没有被同意，则处理的流程前进到步骤 S228，在该步骤中 CPU21 通知许可服务器价格没有被同意。

如上所述对由客户机 1 执行的处理，许可服务器 4 执行由图 33 所示的流程图表示的处理。

如图中所示，流程图开始于步骤 S241，在该步骤中用在许可服务器 4 中的 CPU21 接收来自客户机 1 的许可购买请求。如上所述，这样的请求在图 32 所示的流程图中的步骤 S222 由客户机 1 发送。接着，在下一个步骤 S242，CPU21 从存储单元 28 中读出将由用户购买的许可的价格，并向客户机 1 发送该价格。

如上所述，响应于公开的价格，客户机 1 发送是否同意该价格的判断的结果。

随后，在下一个步骤 S243，用在许可服务器 4 中的 CPU21 基于从客户机 1 接收到的判断的结果确定客户机 1 是否同意该价格。如果价格被同意，处理的流程前进到步骤 S244，产生包括表示购买内容的许可的消息的标志，通过使用它自己的密钥在标志中放入数字签名并向客户机 1 发送该标志。如上所述，在图 32 所示的步骤 S227 中以这种方式发送的标志记录在使用在客户机 1 中的

存储单元28中的内容里。

如果在步骤S243用在许可服务器4中的CPU21确定价格没有被客户机1同意，则跳过步骤S244的处理。即，在这种情况下，最终不执行购买许可的处理。因此，没有标识发送到客户机1。

图34是在步骤S244表示从许可服务器4向客户机1发出的标志的典型结构的图。在该典型结构中，标志包括用户的叶ID、所有权标记（Own）和数字签名Sigs（叶ID，Own），该数字签名基于许可服务器4的密钥S从叶ID和所有权标记中产生。

应当注意到，该标志只对发送到指定用户的指定内容有效。因此，如果指定内容被复制，复制内容中的标记是无效的。

以这种方式，即使内容与许可分离并且使用条件与许可相关，也有可能按照对各个内容的使用情况提供服务。

接着，说明分组。多个装置和介质集中成一组，在这些设备中内容能够以高的自由度交换。这样的一组的形成叫做分组。通常，分组形成包括设备和介质的组，这些装置和介质由个人所有。传统上，分组也包括为每个组设置组密钥的操作。然而，通过把集中成组的多个装置和介质与公共许可相连来分组能简单地完成。

另外，分组能够通过预先为装置分类来执行。这种分组按照下文来说明。

在这种情况下，用户需要预先在服务器中对将被分组的装置的证明来分类。分类这样的证明的处理参照图35和36的流程图说明。

首先，分类客户机，即将被分组的设备的证明的处理参照图35的流程图说明。如图中所示，流程图开始于步骤S261，在该步骤中使用在客户机1中的CPU21产生它自己的证明作为将被分组的设备的证明。该证明包括它自己的披露的密钥。

接着，在下一个步骤S262，CPU21按照由用户向输入单元26键入的输入接入内容服务器3。随后，在下一个步骤S263，在步骤S261产生的证明，被发送到内容服务器3。

应当注意到从许可服务器4接收到的证明也象上述证明一样被使用。

上述处理由所有要分组的设备执行。

参照图36所示的流程图，随后的描述说明了由内容服务器3执行的对证

明分类的处理，该证明通过如图 35 所示的流程图所表示的由客户机 1 执行的分类证明的处理来产生。

如图中所示，流程图开始于步骤 S271，在该步骤中用在内容服务器 3 中的 CPU21 从客户机 1 接收证明。接着，在下一个步骤 S272，证明在存储单元 28 中分类。

对每个将被分组的装置执行上述处理。结果，如图 37 所示包含每一组的设备的证明在用于内容服务器 3 中的存储单元 28 中分类。

在图 37 所示的例子中，证明 C11 至 C14 按照组 1 的证明来分类。这些证明 C21 至 C23 分别包括对应的披露的密钥 K_{P11} 至 K_{P14}。

借助于相同的方法，证明 C21 到 23 按照组 2 的证明来分类。这些证明 C21 至 C23 分别包括相应的披露的密钥 K_{P2} 至 K_{P23}。

当属于一组的装置的用户请求提供内容时，内容服务器 3 用包含这样一组的每个装置分类的证明执行图 38 所示的流程图所表示的处理。

如图中所示，流程图开始于步骤 S281，在该步骤中，用在内容服务器 3 中的 CPU21 执行鉴别该组证明的处理，该组的证明从在存储单元 28 中分类的证明中选择。

如上文中参照图 29 和 30 所描述的，在该鉴别处理中，EKB 通过使用基于包含在证明中的装置的叶 ID 的标记来追踪。EKB 已经由许可服务器 4 向内容服务器 3 分配。鉴别处理除去取消的证明。

接着，在下一个步骤 S282，用在内容服务器 3 中的 CPU21 选择被确认为有效的证明作为在步骤 S281 执行的鉴别处理的结果。随后，在下一个步骤 S283，CPU21 通过使用步骤 S282 执行的处理中选择的设备的证明披露的密钥加密内容密钥。接下来，在下一个步骤 S284，CPU21 把在步骤 S283 执行的处理中加密的内容密钥和它的内容一起发送到请求内容显示的分组装置中。

假定图 37 中所示的一组的证明 C14 已经被取消。在这种情况下，在步骤 S283 执行的处理中，有代表性地产生图 39 所示的加密的密钥。

详细地说，在图 39 所示的加密数据中，内容密钥 Kc 已经通过使用证明 C11 的披露的密钥 K_{P11}、证明 C12 的披露的密钥 K_{P12} 或证明 C13 的披露的密钥 K_{P13} 加密。

当从许可服务器 3 接收的内容作为图 38 中流程图表示的处理的结果时，

属于该组的装置或客户机执行图 40 所示流程图所表示的处理。

如图 40 所示，流程图开始于步骤 S291，在该步骤中，用在客户机 1 中的 CPU21 接收内容密钥 Kc 和内容，它们是在图 38 所示的流程图的步骤 S284 执行的处理中由内容服务器 3 发送的。内容已经通过使用内容密钥 Kc 加密，内容密钥 Kc 已经通过使用由以上描述的装置所保有的披露的密钥加密（参照图 39）。

接着，在下一个步骤 S292，CPU 通过使用客户机 1 所拥有的密钥解密内容密钥 Kc，Kc 已经在步骤 S291 执行的处理中被接收并为客户机 1 所预定。CPU21 接着使用解密的内容密钥对内容解密。

例如，把对应于图 39 中所示的证明 C11 的装置作为例子。装置通过使用它自己对应于披露的密钥 K_{P11} 的密钥解密内容密钥 Kc。接着装置使用解密的内容密钥 Kc 来对内容解密。

相同的处理对与证明 C12 和 C13 相关的装置执行。与取消的证明 C14 相关的装置不接收由加在内容中的它自己的披露的密钥加密的内容密钥 Kc。因此，装置不能通过使用它自己的密钥解密内容密钥 Kc，从而不能通过使用解密的内容密钥 Kc 解密内容。

如上所述，装置关于内容密钥，即关于内容分组。但是，装置是按照许可密钥即许可分组的。

如上所述，装置能够不使用下文所述的指定组密钥或 ICVs（完整检测值）被分组。这种分组适用于小规模的组。

按照本发明，许可能够被检出、登记、移动或复制。然而，这些操作必须按照由 SDMI 确定的规则。

参照图 41 和 42 所示的流程图，接下来的描述说明了通过使用这样的客户机检出许可的处理。

参照图 41 所示的流程图，描述开始于由客户机执行的检出向另一个客户机的许可的处理。如图中所示，流程图开始于步骤 S301，在该步骤中，用在客户机 1 中的 CPU21 读出将被检出的许可的检出操作数（N1）。检出操作数（N1）包含在图 8 所示的使用条件中。从而，检出操作数（N1）从使用条件中读出。

接着，在下一个步骤 S302，用在客户机 1 中的 CPU21 读出将被检出的许可的检出操作的最大数（N2）。在这种情况下，检出操作的检出最大数（N2）

也从使用条件中读出。

随后，在下一个步骤S303，CPU21比较在步骤S301读出的检出操作数(N1)和在步骤S302读出的检出操作的最大数（N2）从而形成检出操作数（N1）是否大于还是小于检出操作的最大数（N2）的判断。

如果检出操作数（N1）小于检出操作最大数（N2），处理的流程前进到步骤S304，在该步骤中CPU21从合作装置那里获取合作装置的叶密钥，该合作装置是用作检出目的地的客户机。与用作检出目标的许可ID相关联，获取的叶密钥在存储在存储单元28中的检出列表中分类。

接着，在下一个步骤S305，CPU21对在步骤S301读出的检出操作数（N1）增加1。随后，在下一个步骤S306，CPU21找到基于许可的消息的ICV。ICV将在下文中参照图46至图50进行说明。通过使用ICV，有可能防止许可被仿造。

接着，在下一个步骤S307，CPU21加密作为检出目标的许可和在步骤S306通过使用客户机1本身拥有的公开的密钥找到的ICV。加密后的许可和加密后的ICV发送到协作装置，在该装置中与EKB和证明一起被复制。接着，在下一个步骤S308，CPU21通过把ICV和协作装置的许可ID和叶密钥相关联对在步骤S306找到的ICV分类在保存在存储单元28中的检出列表上。

如果在步骤S303形成的判断表明检出操作（N1）的数量不小于（例如等于）检出操作数的最大值（N2），则处理的流程前进到步骤S309，在该步骤中CPU21执行差错处理程序。这是因为，检出操作数（N1）不小于检出操作数的最大值（N2），表示许可已经被检出与可允许的检出操作数（N2）一样多次，所以许可不再被检出。从而，在这种情况下，许可不被检出。

参照图42所示的流程图，接下来的描述说明了由客户机执行的接收检出的许可的处理，该许可在图41所示的流程图所表示的检出程序中检出。

图42所示的流程图开始于步骤S321，在该步骤中，用在客户机中的CPU21向协作装置发送由客户机本身所拥有的叶密钥，即客户机1检出许可。与许可ID相关联的叶密钥在步骤S304中保存在协作装置中。

接着，在下一个步骤S322，CPU21从协作客户机1中接收加密的许可和加密的ICV以及EKB和证明。如上文所示，协作客户机1在图41所示流程图的步骤S307中发送加密的许可和加密的ICV以及EKB和证明。

随后，在下一个步骤 S323，CPU21 在存储单元 28 中保存在步骤 S322 接收的加密的许可、加密的 ICV、EKB 和证明。

接收如上所述的检出的许可的客户机 1 按照图 43 所示的流程图所表示的处理，用检出的许可播放内容。

如图中所示，流程图开始于步骤 S341，在该步骤中用在客户机 1 中的 CPU21 找到用户键入到输入单元 26 的命令所指定的内容的 ICV，该内容即是将被播放的内容。随后，在下一个步骤 S342，CPU21 通过使用包含在证明中的披露的密钥解密存在存储单元 28 中的加密的 ICV。

接着，在下一个步骤 S343，CPU21 形成在步骤 S341 找到的 ICV 是否与 ICV 匹配的判断，后一 ICV 在步骤 S342 执行的处理中读出并解密。前者与后者匹配表示许可未被伪造。在这种情况下，处理的流程前进到步骤 S344，在该步骤中 CPU21 执行播放内容的处理。

如果在步骤 S343 形成的判断结果表明两个 ICV 不互相匹配，则恐怕许可已经被伪造。在这种情况下，处理的流程前进到步骤 S345，在该步骤中 CPU21 执行错误处理程序。也就是说，内容不能通过使用该许可而被播放。

参照图 44 所示的流程图，接下来的描述说明了客户机执行的登记许可的处理，该许可如上所述检出给另一个客户机 1。

如图中所示，流程图开始于步骤 S361，在该步骤中用在客户机中的 CPU21 接收协作装置叶密钥和将被登记的许可 ID。协作装置是客户机 1，它恢复或登记许可。接着，在下一个步骤 S362，CPU21 形成在步骤 S361 获得的将被登记的许可是否是由客户机本身给协作装置检出的许可的判断。该判断基于 ICV、叶密钥和许可 ID，它们在图 41 所示的流程图的步骤 S308 执行的处理中保存在存储单元 28 中。也就是说，CPU21 确定在步骤 S361 接收的 ICV、叶密钥和许可 ID 是否已经在保存在存储单元 28 中的检出表中分类。如果它们已经在检出表中被分类，CPU21 确定将被登记的许可是客户机本身给协作装置检出的许可。

如果将被登记的许可是由客户机本身给协作装置检出的许可，则处理的流程前进到步骤 S363，在该步骤中 CPU21 提出删除协作装置的 EKB、证明和许可的请求。如在下文中将描述的，在图 45 所示的流程图的步骤 S383 协作装置按照请求删除许可、EKB 和证明。

接着，在下一个步骤 S364，因为检出的许可被登记，CPU21 对检出操作数（N1）减1。

随后，在下一个步骤 S365，CPU21 形成另一个许可是否已经给协作装置检出的判断。如果给协作装置检出的另一个许可不存在，处理的流程前进到步骤 S366，在该步骤中 CPU21 从检出列表中删除协作装置，该检出列表用于把协作装置按照登记协作装置分类。如果在步骤 S365 形成的判断结果表示给协作装置检出的另一个许可存在，则跳过步骤 S366 的处理。这是因为，其他许可由协作装置登记是在可能性的范围内。

如果在步骤 S362 形成的判断结果表示将被登记的许可不是由客户机本身给协作装置检出的许可，则处理的流程前进到步骤 S367，在该步骤中 CPU21 执行错误处理程序。也就是说，在这种情况下，不执行登记处理，因为许可不是由客户机本身管理的许可。

用户做出的非法复制许可的尝试中，不执行登记处理，因为存储的 ICV 不等于基于在步骤 S361 执行的处理中获得的许可找到的 ICV。

图 45 是表示由客户机 1 执行的发出给另一个客户机登记许可处理请求的处理表示的流程图，另一个客户机执行图 44 所示的流程图表示的许可登记处理。

图45所示的流程图开始于步骤S381，在该步骤中，用在客户机1中的CPU21发送叶密钥和将登记的许可的 ID 给协作装置，该协作装置是执行图 44 所示的流程图所表示的许可登记处理的客户机 1。如上所述，协作装置在步骤 S361 接收叶密钥和许可 ID 并在步骤 S362 基于叶密钥和许可 ID 执行鉴别将被登记的许可的处理。

接着，在下一个步骤 S382，用在客户机 1 中的 CPU21 形成删除许可的请求是否已经从协作装置接收的判断。如前文所述，如果许可是将被登记的正确的许可，协作装置在步骤 S363 执行的处理中提出删除许可、EKB 和证明的请求。如果在步骤 S382 形成的判断的结果表明这样的请求已经被接收，处理的流程前进到步骤 S383，在该步骤中 CPU21 删除许可、EKB 和证明。也就是说，客户机 1 从而变得不再能使用许可。因为，在图 44 所示的流程图的步骤 S364 执行的处理中通过协作装置检出操作数（N1）减1，登记处理结束。

如果在步骤 S382 形成的判断结果表示没有接收这样的申请，则处理的流

程前进道步骤 S384，在该步骤中 CPU21 执行错误处理程序。也就是说，在这种情况下，由于比如 ICV 中的差异这样的原因，不能执行登记处理。

到现在为止已经说明了检出处理和登记处理。还可以执行复制或移动许可的处理。

接下来的描述说明了产生许可的 ICV（完整的检测值）的处理，把 ICV 和许可相关联并形成许可是否已经通过 ICV 的计算被伪造的判断的处理，从而防止许可被伪造。应当注意到能够对内容应用相同的处理。

许可的 ICV（完整的检测值）通过如下的典型的许可的散列函数的应用被计算：

ICV=hash（Kicv，L1，L2，…）

其中符号 Kicv 表示 ICV 产生密钥，而信号 L1 和 L2 每个都表示许可上的信息。许可的重要信息的 MAC（消息鉴别码）被用作由 L1 和 L2 表示的信息。

图 46 是表示典型的通过使用 DES 加密处理结构的 MAC 值产生的图。从图 46 所示的结构很明显看出处理的消息被分成 8 字节的单元。在随后的描述中，分开的信息指 M1、M2，…和 MN。首先，初始值 IV 和 M1 提供到处理单元 24-1A，执行专用的逻辑和处理，产生专用的逻辑和 11。接着，专用的逻辑和 11 提供到 DES 加密单元 24-1B，以通过使用密钥 K1 加密 11 产生加密结果 E1。随后，E1 和 M2 提供到处理单元 24-2A，以执行专用的逻辑和处理，产生专用的逻辑和 12。接着，专用的逻辑和 12 提供给 DES 加密单元 24-2B，以通过使用密钥 K1 加密 12 从而产生加密结果 E2。因此，这些操作被重复地执行来加密所有的消息。最终，由 DES 加密单元 24-NB 产生的结果 EN 是 MAC（消息鉴别码）。

散列函数则应用到这样的许可 MAC 值和 ICV 产生密钥以产生 ICV（完整的检测值）。例如，在许可的产生中计算出的 ICV 与从许可重新计算的 ICV 相比较。如果 ICV 彼此匹配，就能确保许可没有被伪造。如果 ICV 彼此不匹配，则许可被确定为已经被伪造。

接下来的描述说明了使用 EKB（使能密钥块）发送密钥 Kicv 以产生许可的 ICV（完整的检测值）的结构。在该结构中，通过使用 EKB 加密的信息数据被用作密钥 Kicv 以产生许可的 ICV（完整的检测值）。

准确地说，图 47 和 48 每个图都是表示使用 EKB（使能密钥块）分配用于

产生共用许可的 ICV（完整的检测值）的密钥 Kicv，以在向多个设备发送许可时形成许可是否已经被伪造的判断的典型结构。更明确地说，图 47 是表示典型的向设备 0、1、2 和 3 分配用于产生许可的 ICV（完整的检测值）的可解密的密钥 Kicv 的图。而图 48 是表示典型的向设备 0、1 和 2 但不向已经被取消的设备 3 分配用于产生许可的 ICV（完整的检测值）的可解密的密钥 Kicv。

在图 47 所示的典型的分配中，产生能够被解密的加密的 EKB（使能密钥块）。EKB 被用于向设备 0、1、2 和 3 发送数据 Enc（K（t）00，Kicv）和更新后的节点密钥 K（t）00。数据 Enc（K（t）00，Kicv）是通过使用更新后的节点密钥 K（t）00 对检测值产生密钥 Kicv 加密的结果。节点密钥 K（t）00 已经通过使用节点密钥和叶密钥被更新，设备 0、1、2 和 3 每个都拥有节点密钥和叶密钥。如图 47 的右侧所示，首先每个设备 0、1、2 和 3 解密 EKB 以获得更新后的节点密钥 K（t）00。接着，更新后的节点密钥 K（t）00 被用于解密加密后的检测值产生密钥 Enc（K（t）00，Kicv）以获得检测值产生密钥 Kicv。

即使 EKB 由设备所接收，其他的设备 4、5、6、7 等每个都不能通过处理 EKB（使能密钥块）和通过使用每个设备所具有的节点密钥和叶密钥获得更新后的节点密钥 K（t）00。因此，检测值产生密钥能够只被发送到具有高安全性的授权设备。

图 48 是表示因为密钥已经泄漏，属于一组在图 12 中用虚线围起来的设备 3 已经被取消，从而 EKB（使能密钥块）产生并只被分配到该组中其他设备即设备 0、1 和 2 的情况的图。EKB（使能密钥块）只能够由设备 0、1 和 2 被解密。图 48 所示的 EKB（使能密钥块）和数据 Enc（K（t）00，Kicv）被分配。如前文所述，数据 Enc（K（t）00，Kicv）是通过使用节点密钥 K（t）00 加密检测值产生密钥 Kicv 的结果。

在图 48 的右侧示出了解密的程序。如图所示，首先设备 0、1 和 2 每个使用本身所具有的叶密钥或节点密钥通过执行对接收到的 EKB（使能密钥块）解密的处理获得更新后的密钥 K(t)00。接着，检测值产生密钥 Kicv 通过基于更新后的节点密钥 K(t)00 被解密获得。

图 12 所示的组中的其他设备 4、5、6 等的每一个，即使相同的 EKB（使能密钥块）分配给其他设备，都不能够通过使用自己的叶密钥和节点密钥获得更新后的节点密钥 K（t）00。同样说来，即使相同的 EKB（使能密钥块）被

分配给该设备，取消后的设备 3 也不能通过使用它自己的叶密钥和节点密钥获得更新后的密钥 K（t）00。因此，只有授权后的设备能够解密并使用检测值产生密钥 Kicv。

以这种方式，通过利用检测值产生密钥 Kicv 通过 EKB 的使用的分配，分配的数据量能够减少并有可能安全地只向授权的能够解密检测值产生密钥 Kicv 的部分分配检测值产生密钥 Kicv。

通过使用这样的许可的 ICV（完整的检测值），有可能避免 EKB 和加密的许可的非法复制。假定介质 1 被用于如图 49A 所示与能被用于获取它们的许可密钥的 EKB（使能密钥块）一起保存许可 L1 和 L2。让保存在介质 1 中的内容复制到介质 2 中。在这种情况中可以复制 EKB 和许可。能够解密 EKB 的设备也将能够使用许可。

在图 49B 所示的结构中，完整的检测值 ICV（L1，L2）保存在与保存在其中的许可相关联的每个介质中。应当注意到 ICV（L1，L2）是许可 L1 和 L2 的完整的检测值并如下所示通过对许可 L1 和 L2 应用散列函数计算：

ICV=hash（Kicv，L1，L2）

在图 49B 所示的结构中，保存在介质 1 信息包括许可 1 和 2 以及完整的检测值 ICV（L1，L2），它通过向许可 L1 和 L2 应用散列函数被计算。另一方面，保存在介质 2 中的信息包括许可 1 和完整的检测值 ICV（L1），它通过向许可 L1 应用散列函数被计算。

在该结构中，假定{EKB，许可 2}从介质 1 向介质 2 复制。在这种情况下，新的许可检测值 ICV（L1，L2）能够在介质 2 中产生。新许可检测值 ICV（L1、L2）不用于存储在介质 2 中的 Kicv（L1）。因此很明显新的许可检测值 ICV（L1，L2）能够被用于通过伪造或非法复制操作在介质 2 中保存新的许可。然而在用于播放保存在介质 2 中的信息的装置中，产生并保存的 ICV 能够先于播放步骤的步骤中被检测，以形成 ICV 是否互相匹配的判断。如果产生的 ICV 被确定为不与保存的 ICV 匹配的 ICV，则不执行播放操作。以这种方式，在该结构中，有可能防止通过伪造或执行非法复制操作获得的许可被播放。

另外，为了进一步加强安全度，有可能设计一种结构，其中许可的 ICV（完整的检测值）在包含可写入计数器值的数据基础上产生。具体地说，在该结构中，许可的 ICV（完整的检测值）按照如下形式计算：

ICV=hash（Kicv，计数器+1，L1，L2，…）

其中符号（计数器+1）表示计数器的值在 ICV 每次更新时增加 1。应当注意计数器的值需要保存在该结构中的安全的存储器中。

而且，在许可的 ICV（完整的检测值）不能与许可保存在相同的介质中的结构中，许可的 ICV（完整的检测值）可以保存在与保存许可的介质不同的介质中。

假定许可保存在没有抵御非法复制操作保护的介质中。这样的介质的例子是只读存储器和普通 MO 盘。在这种情况下，如果 ICV（完整的检测值）也保存在相同的介质中，确实在有可能的范围内未授权的用户能够更新 ICV。因此恐怕不能确保 ICV 的安全性。为了解决该问题，ICV 保存在主机的安全介质中并用于控制复制该许可的操作。复制操作的例子是登记、检测和移动许可的操作。因此在这样的结构中有可能执行 ICV 的安全管理和检测许可的伪造。

图 50 是表示执行上述方案的典型结构的图。在图 50 所示的典型结构中，没有抵御非法复制操作保护的介质 2201 用于保存许可 1 至 3。介质 2201 的例子是只读存储器和普通的 MO 盘。另外，用于这些许可的 ICV（完整检测值）保存在主机中使用的安全介质 2202 中，用户不允许以很高的自由度接入该主机。因此，在该典型结构中，用户被防止非法更新 ICV（完整的检测值）。当介质 2201 安装在其中的设备从介质 2201 播放信息时，例如，作为设备主机或服务器的 PC 可以被构造为从形成介质是否被允许播放的判断来检测 ICV。在这样的结构中，从而有可能防止播放非法复制的或伪造的许可的操作。

另外，本发明提供的客户机也能够用与所谓的个人计算机不同的装置来完成。除所谓的个人计算机之外的装置的例子是 PDA（个人数字助理）、蜂窝电话和游戏终端。

如果处理的一系列步骤由软件来完成，组成软件的程序能够从网络或记录介质安装到包含嵌入的特殊硬件的计算机中或其它类型的计算机，如能够通过执行安装在个人计算机中的各种程序执行各种功能的通用个人计算机中。

与作为客户机或服务器的装置的主要部件分离提供的记录介质被分配给用户以向用户提供记录在介质中的程序。记录介质可以是程序包介质。如图 2 所示，程序包介质的例子是包含软盘的磁盘 41、包含 CD-ROM（只读光盘存储器）和 DVD（数字多功能/视盘）的光盘 42、包含 MD（迷你盘）的磁光盘 43

和半导体存储器 44。不从网络或记录介质中安装程序的话，程序也可以通过在嵌入设备主要部件的记录介质中预先保存程序提供给用户。如图 2 所示，嵌入的记录介质的例子是包括在存储单元 28 中的ROM22 和硬盘。

在本说明书中，描述保存在记录介质中的程序的步骤当然能够按照写入的程序一个步骤接一个步骤连续地执行。但是，应当注意到，步骤并不是必须要连续执行，步骤也可以包括并行或单独执行的处理块。

另外，对执行程序也加密以完成关于安全的处理，从而防止程序本身的处理被分析是理想的。例如，被执行来完成加密过程的程序可以被设计为一个抗干扰模块。

而且，包含在内容的首部中指定允许使用内容的许可的信息不必须是唯一地识别许可的许可 ID。在上述的实施例中，许可 ID 是指定使用内容所需要的许可的信息、指定由某一许可所允许内容使用的信息和用于识别由来自客户机 1 的许可请求所请求的许可的信息。取而代之，关于内容的各种属性信息的列表也可以包含在内容中，并且内容的特征的情况也可以包含在用于指定允许使用的内容的许可中。在这种情况下，包含在内容中属性信息是用于指定允许内容使用的信息和用于按照包含在许可中的条件方程指定由许可所允许使用的内容的信息。许可 ID 是用于唯一地识别许可的信息。以这种方式，内容能够与多个许可相关联，从而内容能够以更灵活的方式被发出。

另外，用于该说明书中的技术术语‘内容交换系统’意味着整个系统包括多个装置。

如上所述，按照本发明提供的信息处理装置和方法和执行信息处理方法的程序，加密的数据能够以高自由度分配并且通过获取与内容分别提供的许可，用户能够使用内容。结果，能够保护版权并能够不妨碍内容的分配收集适当的使用费用。

说 明 书 附 图

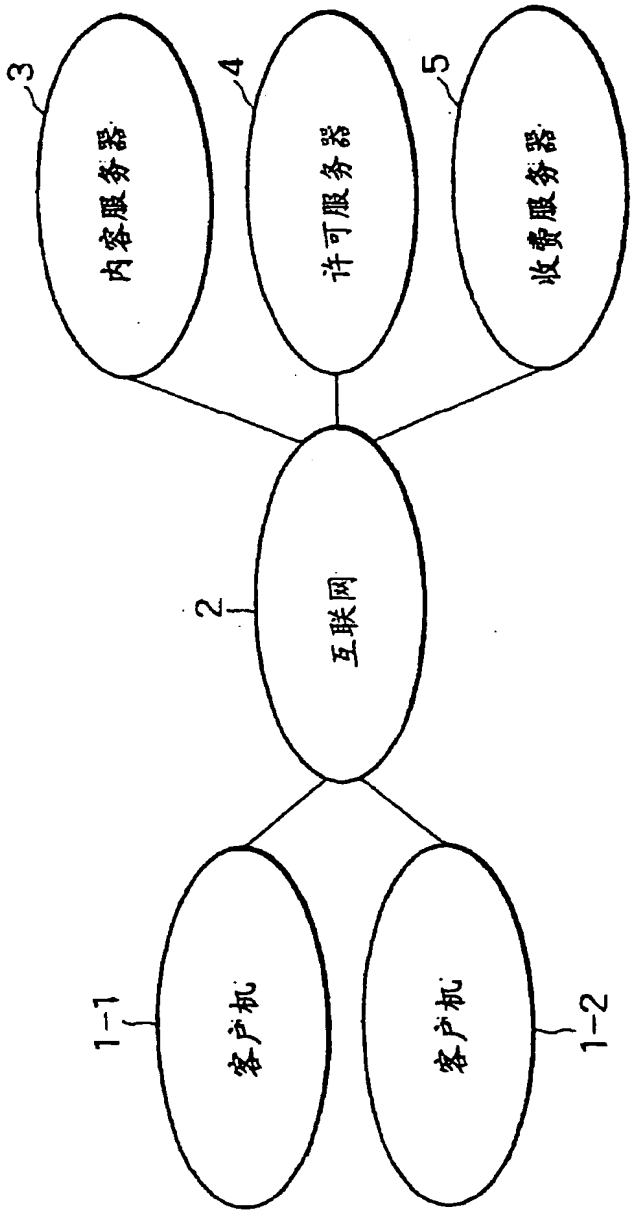


图 1

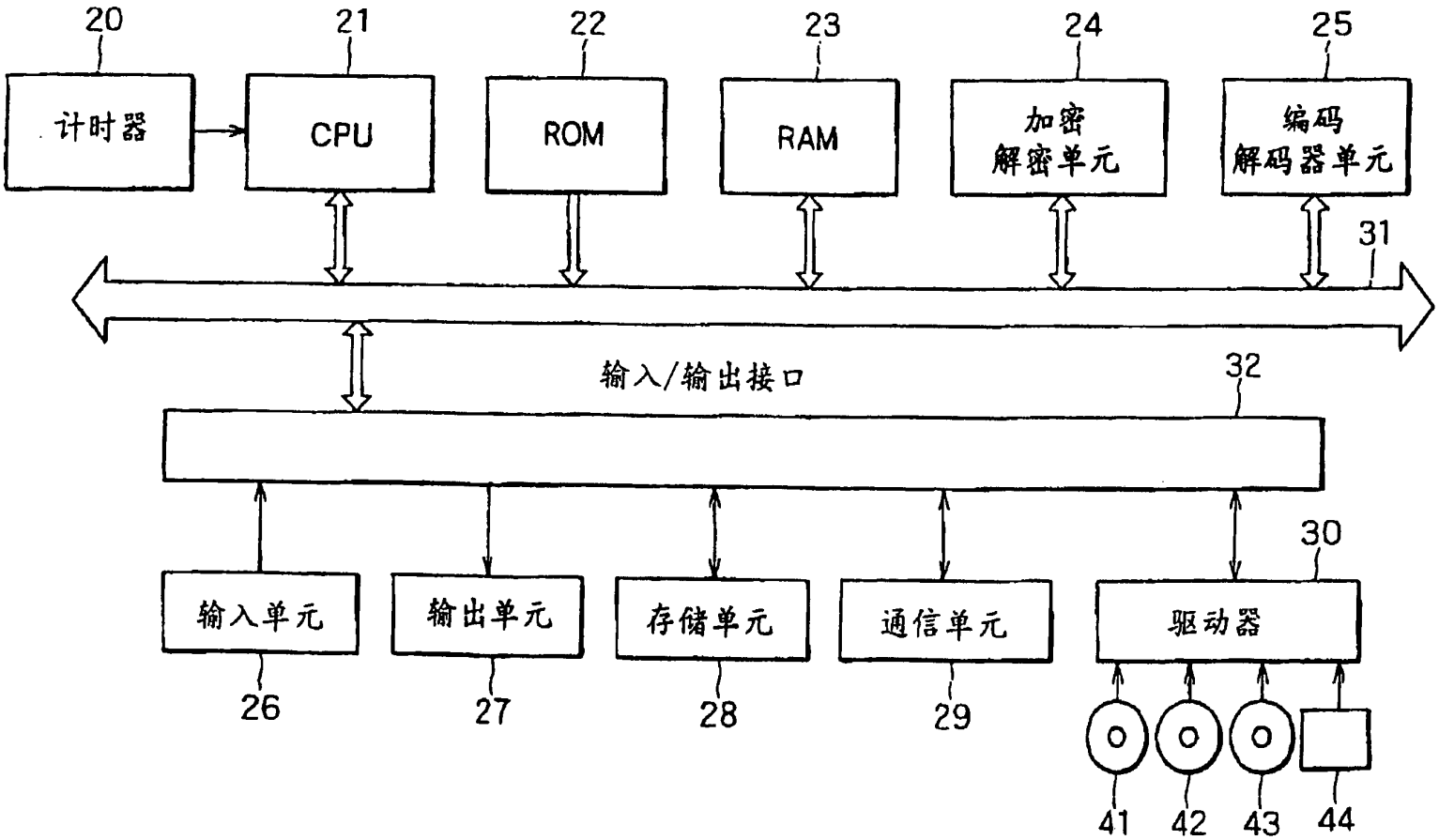

20
21
22
23
24
25
计时器
CPU
ROM
RAM
加密
解密单元
编码
解码器单元
31
输入/输出接口
32
30
输入单元
输出单元
存储单元
通信单元
驱动器
26
27
28
29
41
42
43
44

图 2

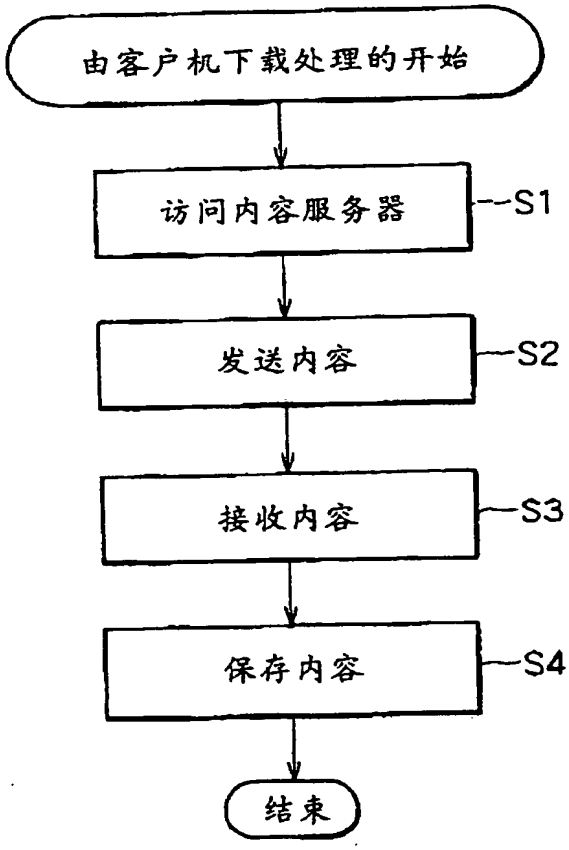


图 3

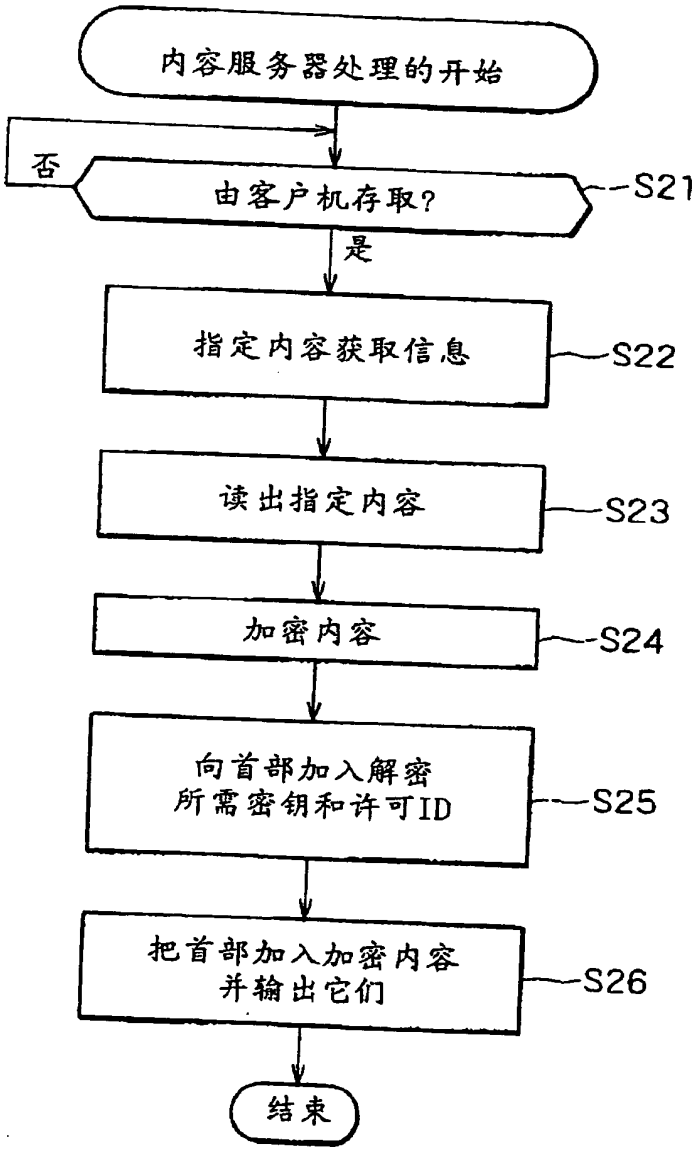

内容服务器处理的开始
否
由客户机存取?
S21
是
指定内容获取信息
S22
读出指定内容
S23
加密内容
S24
向首部加入解密
所需密钥和许可ID
S25
把首部加入加密内容
并输出它们
S26
结束

图 4

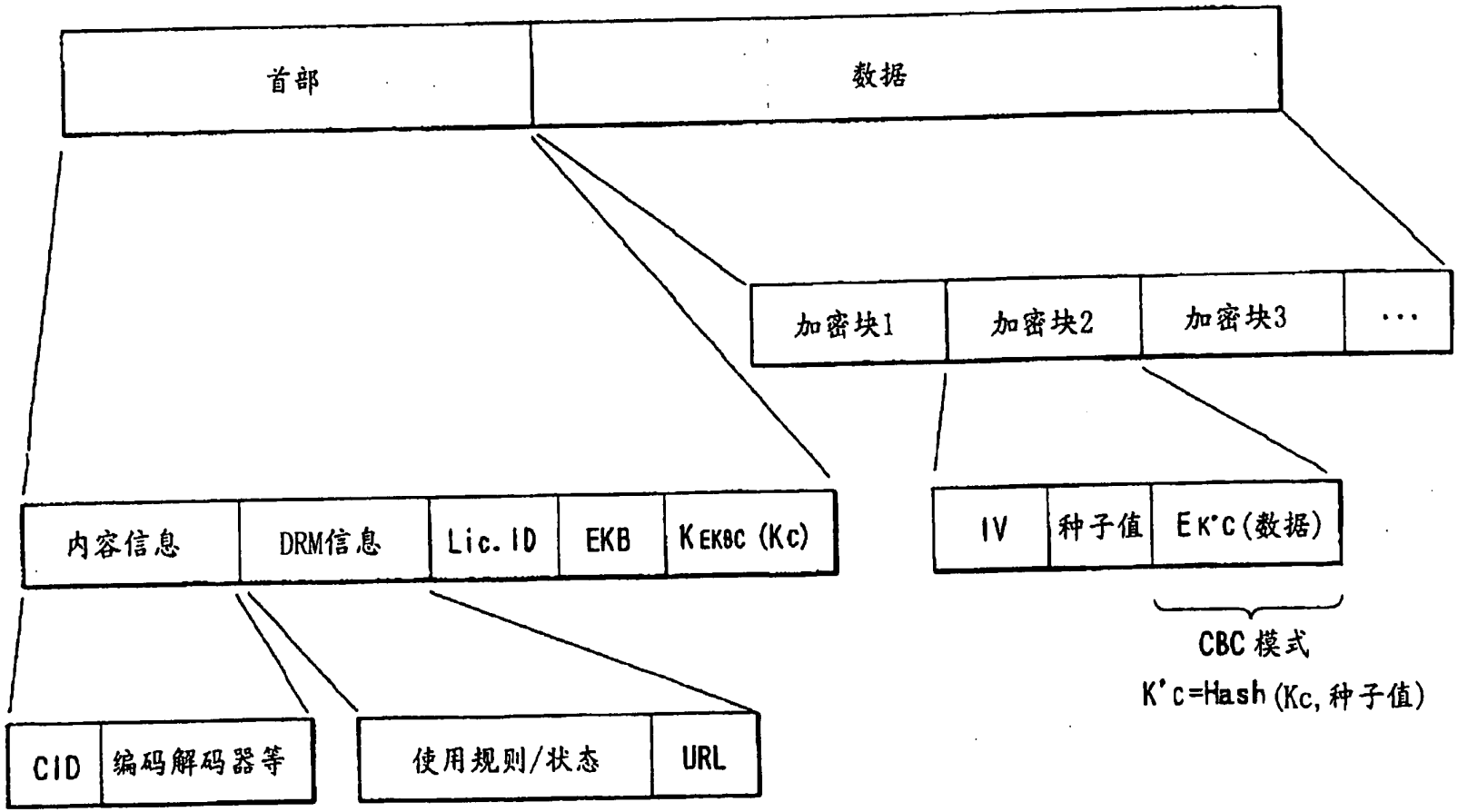

首部
数据
加密块1
加密块2
加密块3
...
内容信息
DRM信息
Lic. ID
EKB
KEKBC (Kc)
IV
种子值
EK'C (数据)
CBC 模式
K'c=Hash (Kc, 种子值)
CID
编码解码器等
使用规则/状态
URL

图 5

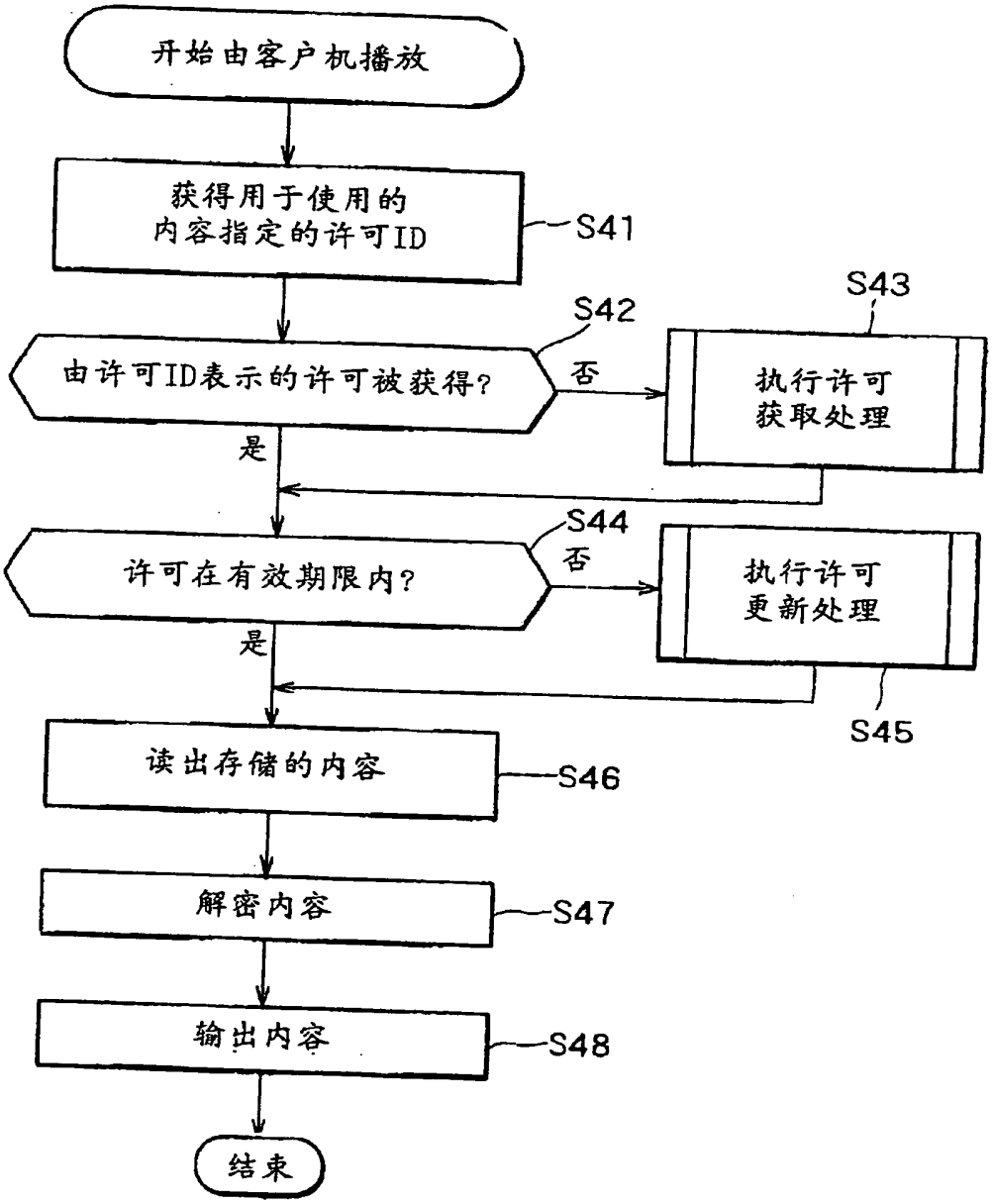

开始由客户机播放
获得用于使用的内容指定的许可ID
S41
S42
由许可ID表示的许可被获得?
否
S43
执行许可获取处理
是
S44
许可在有效期限内?
否
执行许可更新处理
是
S45
读出存储的内容
S46
解密内容
S47
输出内容
S48
结束

图 6

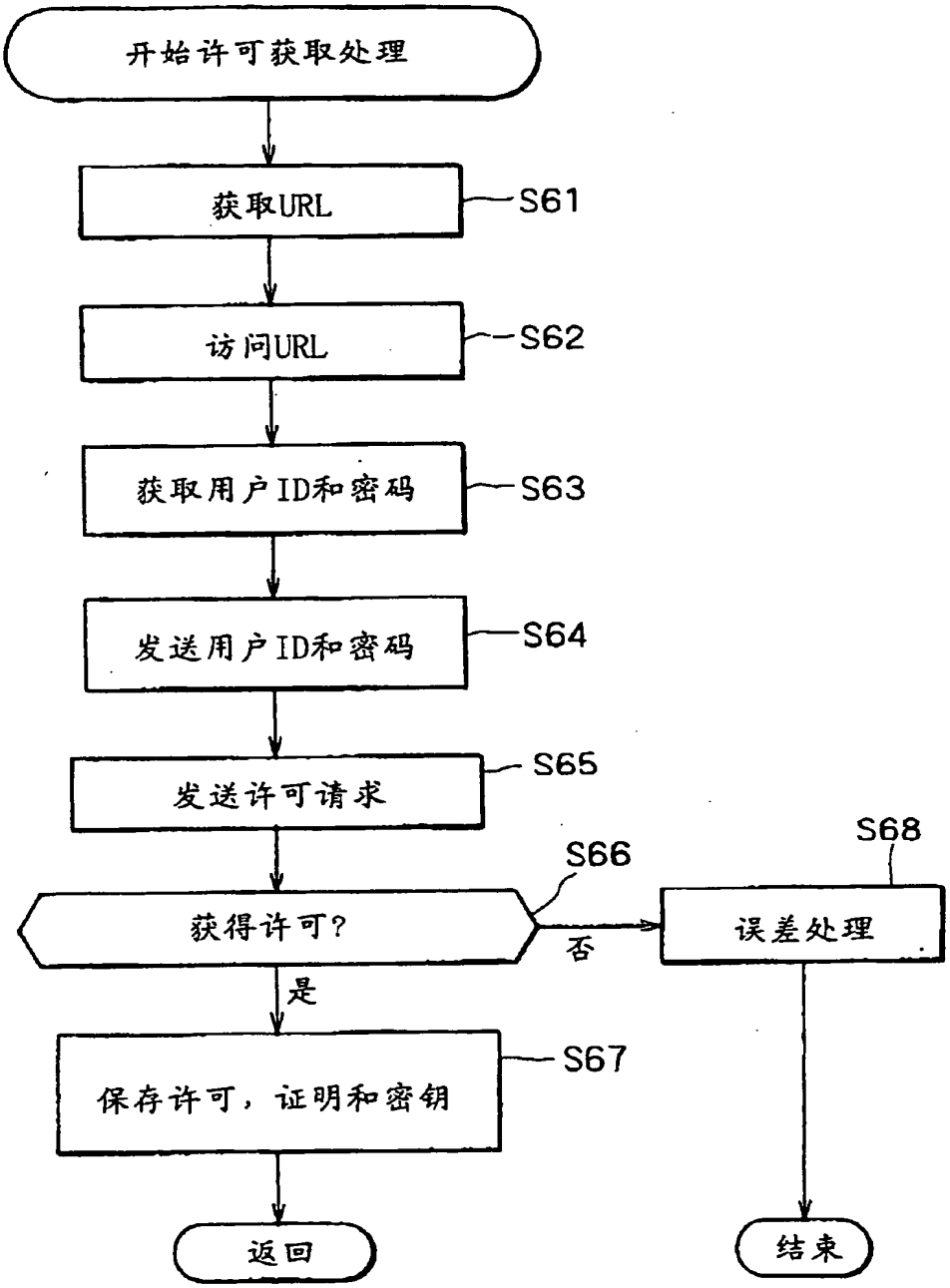

开始许可获取处理
获取URL
S61
访问URL
S62
获取用户ID和密码
S63
发送用户ID和密码
S64
发送许可请求
S65
S66
获得许可?
否
S68
误差处理
是
S67
保存许可，证明和密钥
返回
结束

图 7

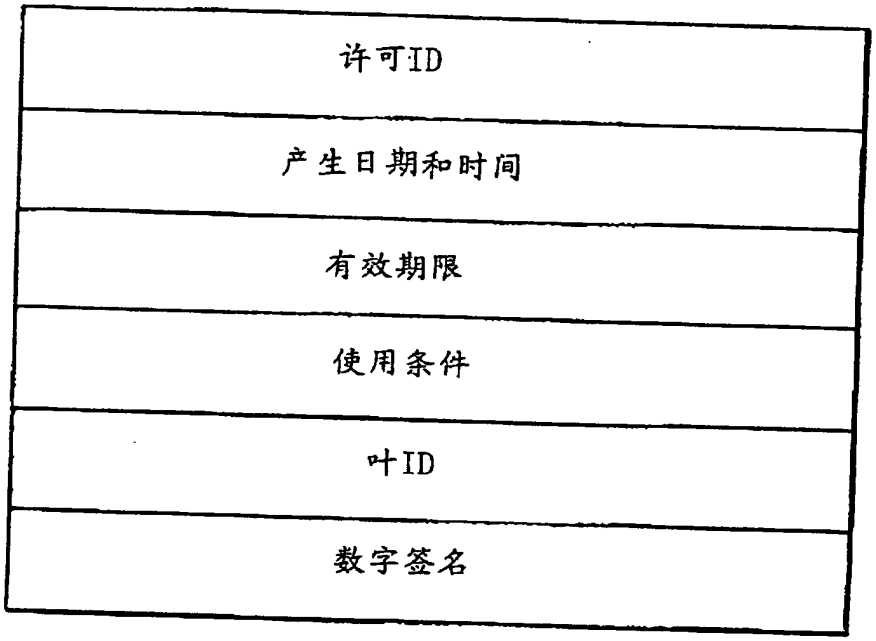


图 8

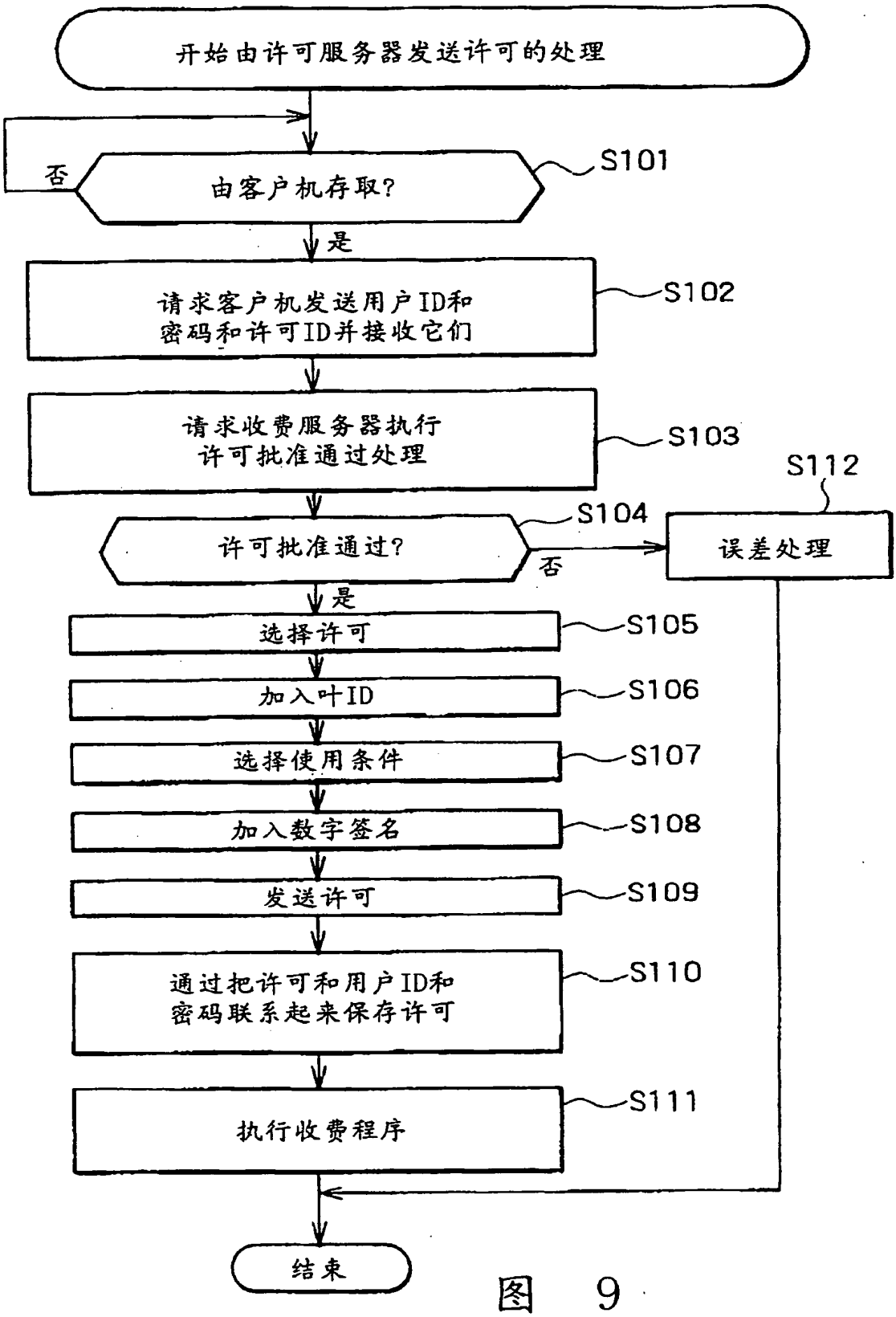

开始由许可服务器发送许可的处理
否
由客户机存取?
S101
是
请求客户机发送用户ID和
密码和许可ID并接收它们
S102
请求收费服务器执行
许可批准通过处理
S103
S112
S104
许可批准通过?
否
误差处理
是
选择许可
S105
加入叶ID
S106
选择使用条件
S107
加入数字签名
S108
发送许可
S109
通过把许可和用户ID和
密码联系起来保存许可
S110
执行收费程序
S111
结束

图 9

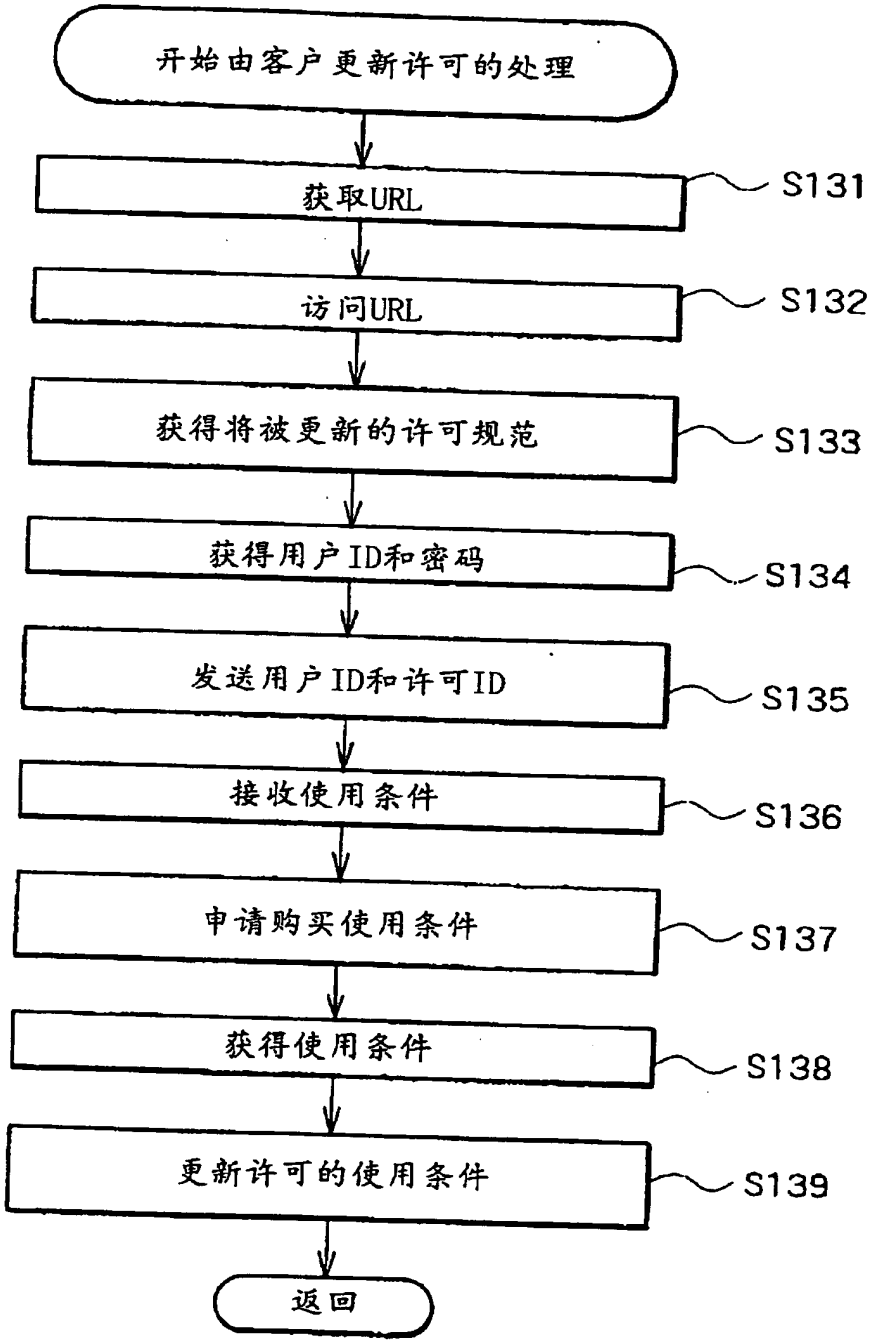

开始由客户更新许可的处理
获取URL
S131
访问URL
S132
获得将被更新的许可规范
S133
获得用户ID和密码
S134
发送用户ID和许可ID
S135
接收使用条件
S136
申请购买使用条件
S137
获得使用条件
S138
更新许可的使用条件
S139
返回

图 10

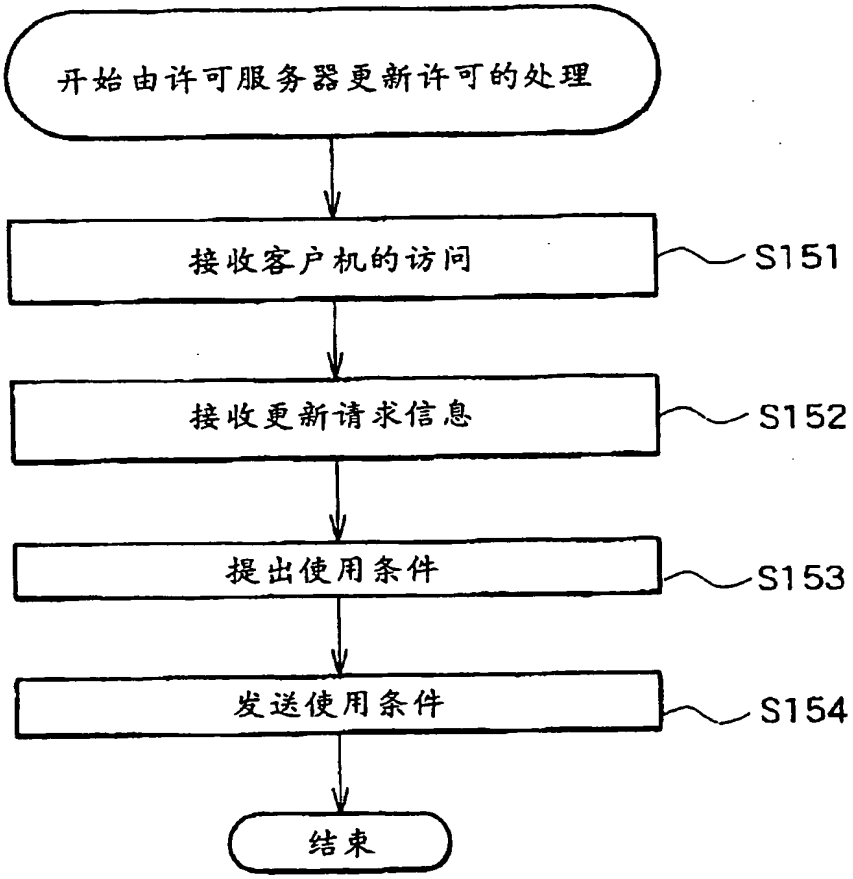

开始由许可服务器更新许可的处理
接收客户机的访问
S151
接收更新请求信息
S152
提出使用条件
S153
发送使用条件
S154
结束

图 11

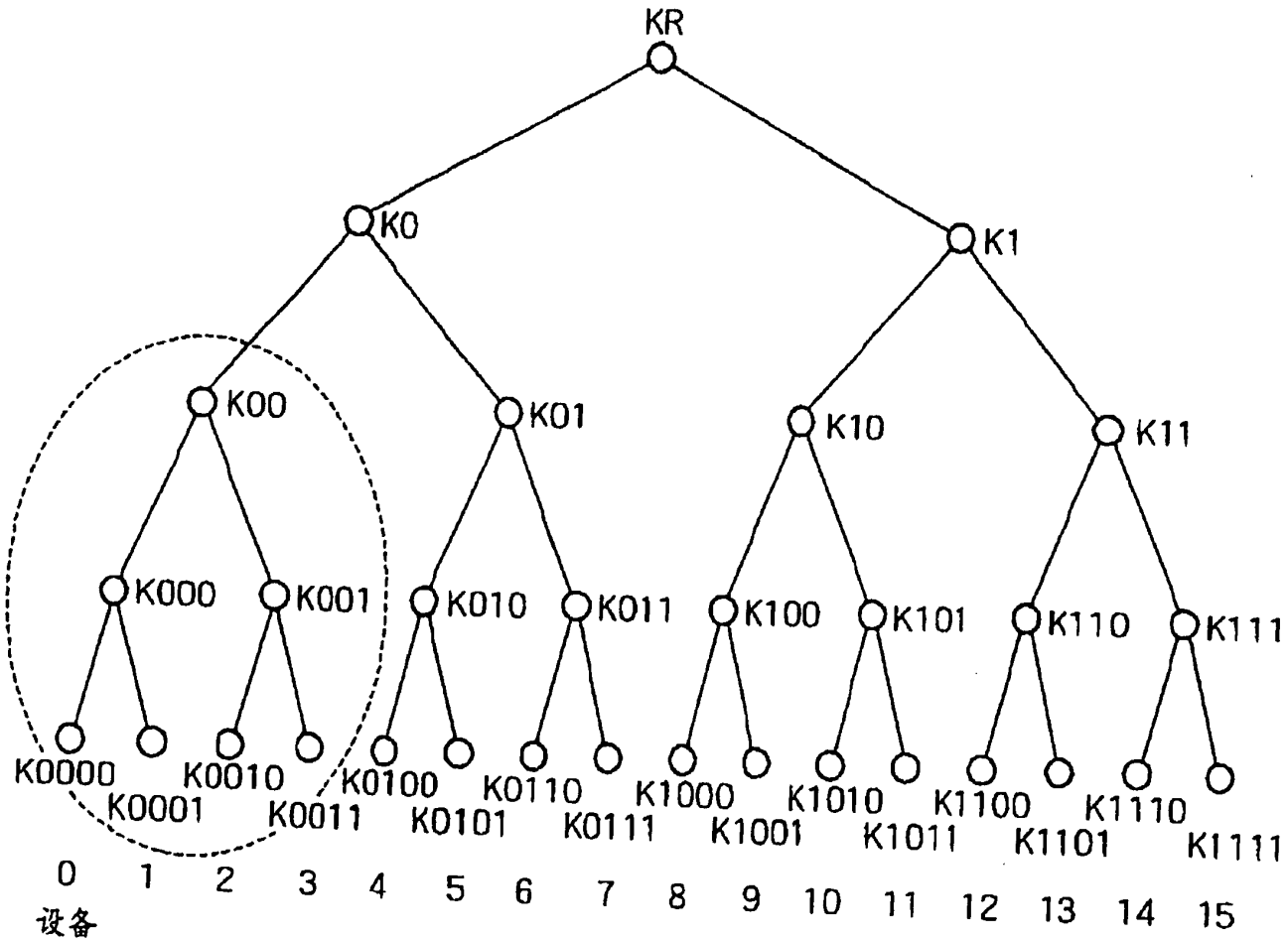

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
设备

图 12

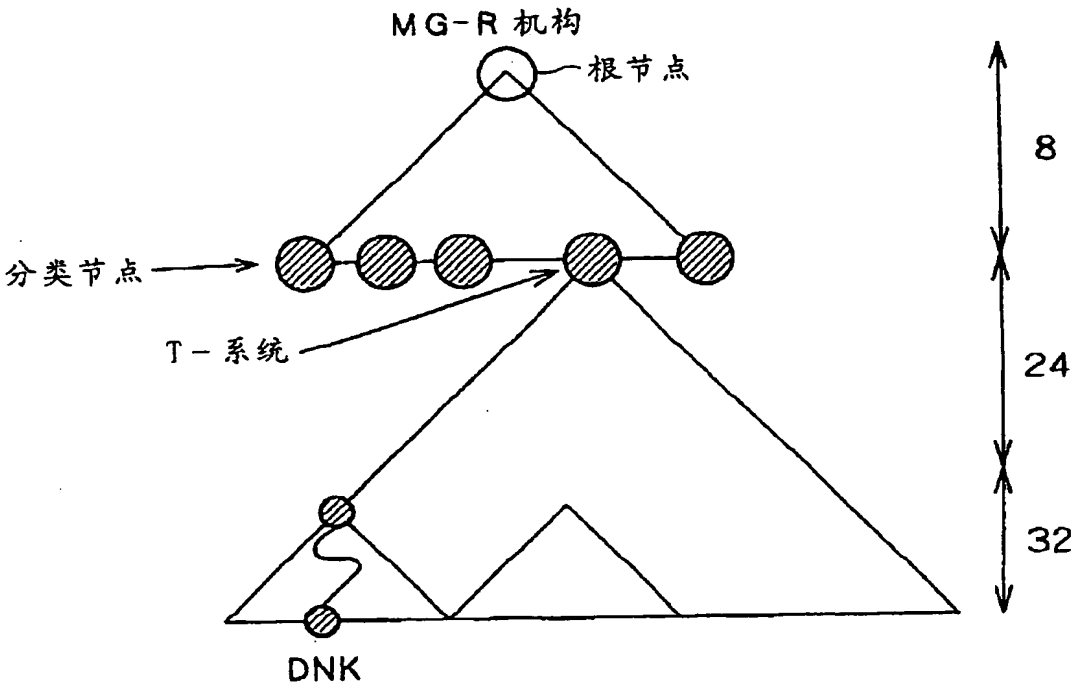


图 13

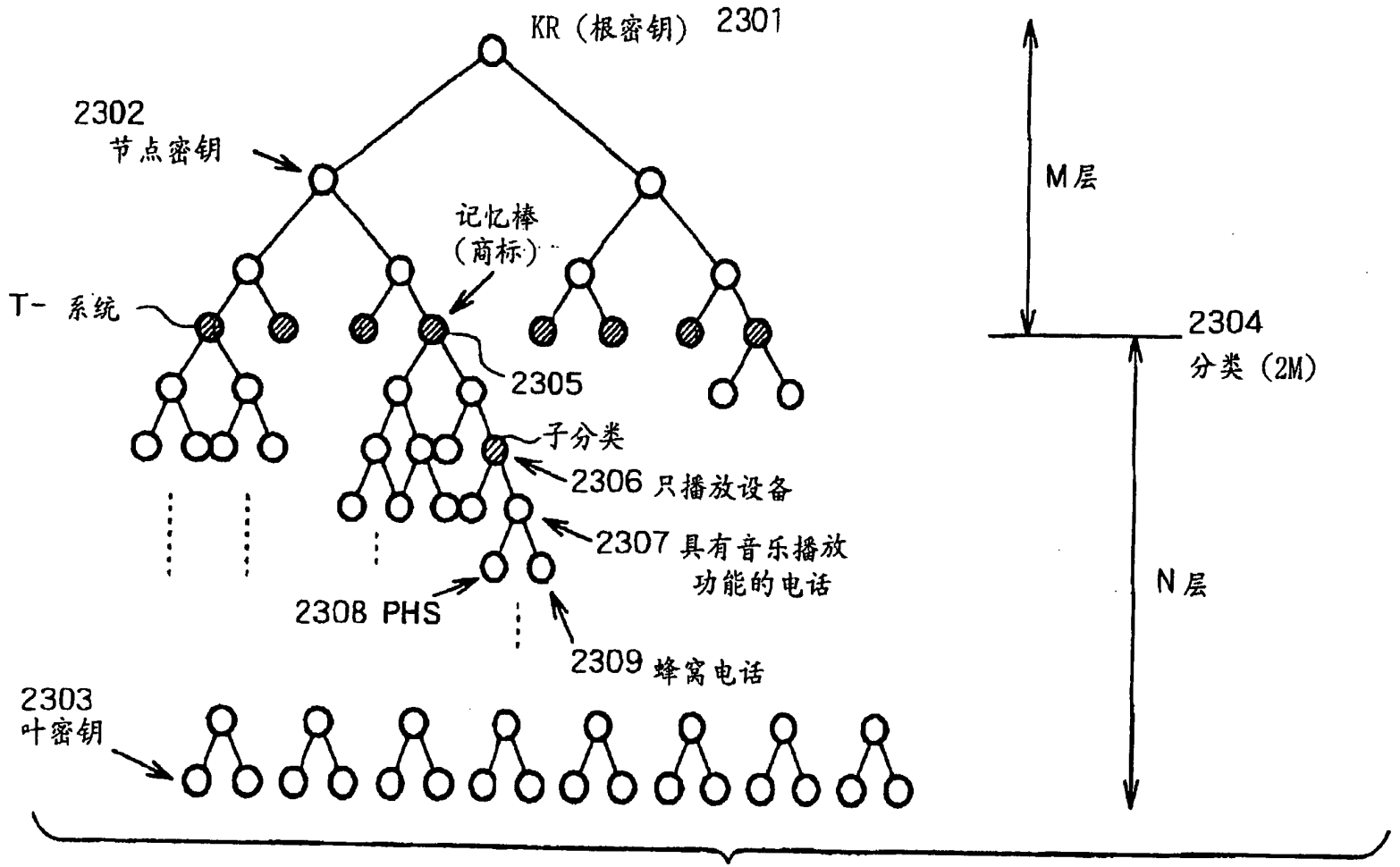

KR（根密钥） 2301
2302
节点密钥
记忆棒
（商标）
T- 系统
2305
子分类
2306 只播放设备
2307 具有音乐播放
功能的电话
2308 PHS
2309 蜂窝电话
2303
叶密钥
M层
2304
分类（2M）
N层

图 14

EKB（使能密钥块）
把方案t的节点密钥
发送到设备0，1和2

形式:t	
索引	加密密钥
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

图 15A

EKB（使能密钥块）
把方案t的节点密钥
发送到设备0，1和2

形式：t	
索引	加密密钥
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

图 15B

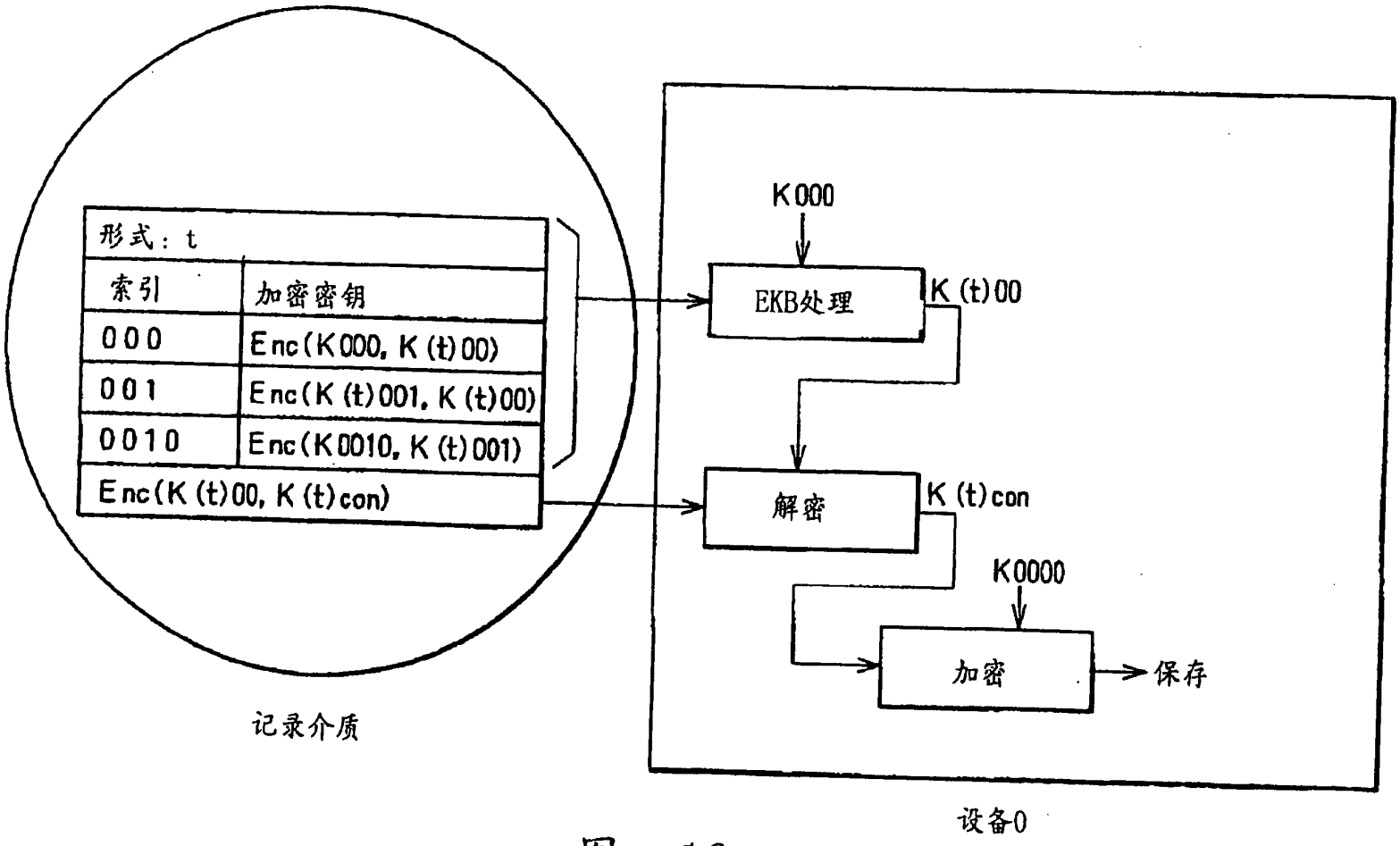

形式：t
索引
加密密钥
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)
记录介质
K000
EKB处理
K(t)00
解密
K(t)con
K0000
加密
保存
设备0

图 16

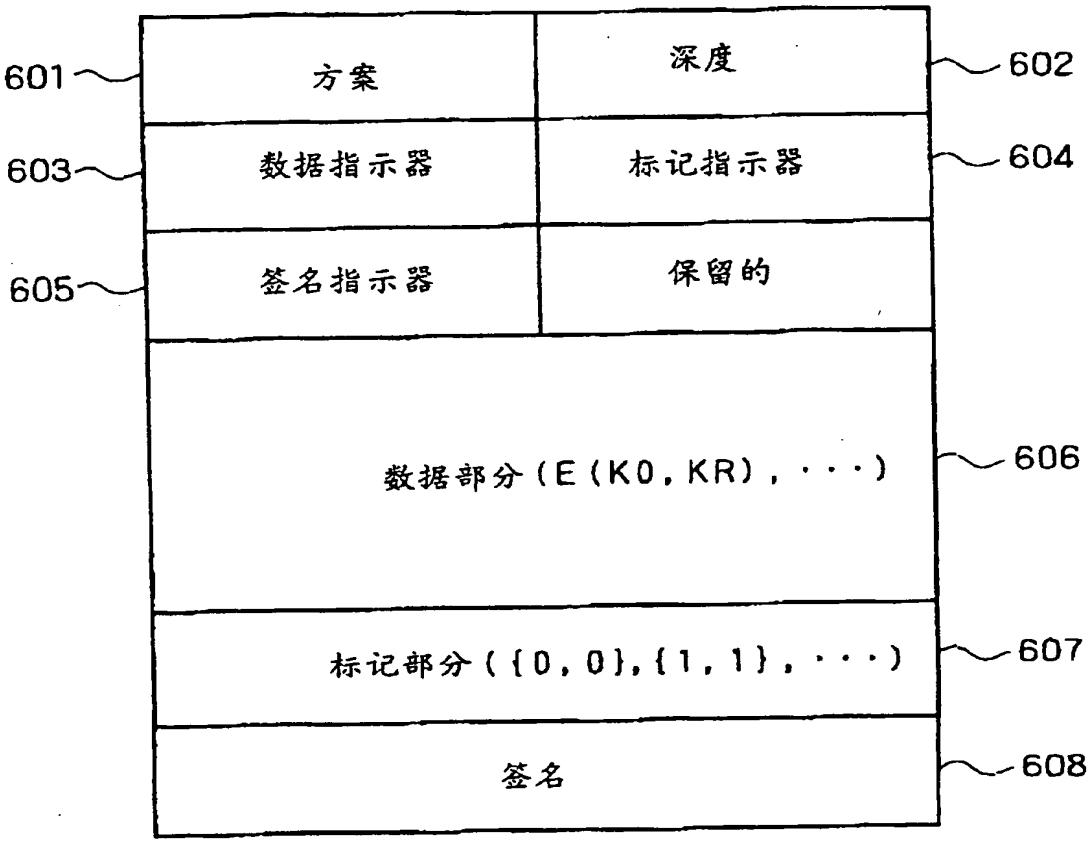

601
方案
深度
602
603
数据指示器
标记指示器
604
605
签名指示器
保留的
数据部分（E（K0，KR），・・・）
606
标记部分（{0，0}，{1，1}，・・・）
607
签名
608
EKB

图 17

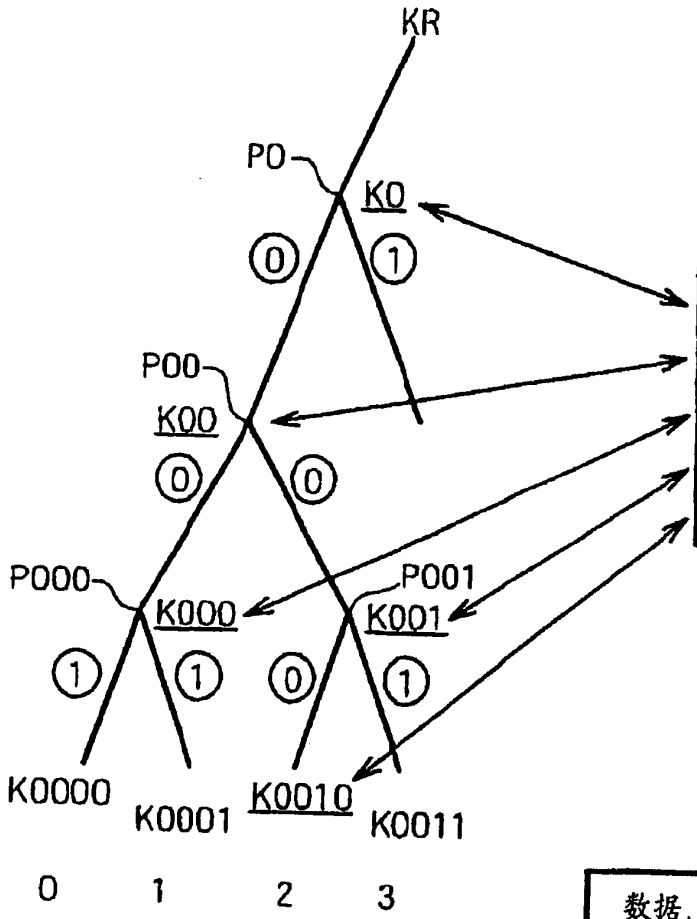


图 18A

EKB（使能密钥块）

向设备0、1和2发送模式t的节点密钥

顶节点地址：KR	
数据（加密密钥）	标记
Enc(K(t)0, K(t)R)	{0, 1}
Enc(K(t)00, K(t)0)	{0, 0}
Enc(K000, K(t)00)	{1, 1}
Enc(K(t)001, K(t)00)	{0, 1}
Enc(K0010, K(t)001)	{1, 1}

图 18B

{L标记，R标记}

L标记和R标记
每个0表示存在数据
而1表示不存在数据

数据：Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), …
标记：{0, 1}, {0, 0}, {1, 1}…

图 18C

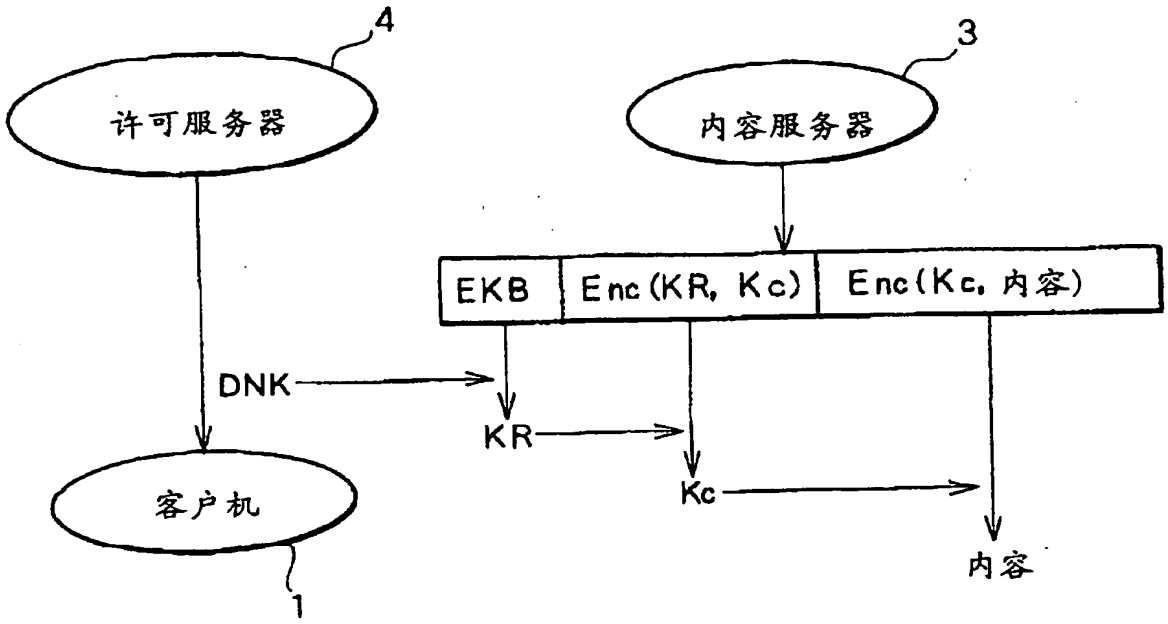

4
许可服务器
3
内容服务器
EKB
Enc(KR, Kc)
Enc(Kc, 内容)
DNK
KR
Kc
内容
客户机
1

图 19

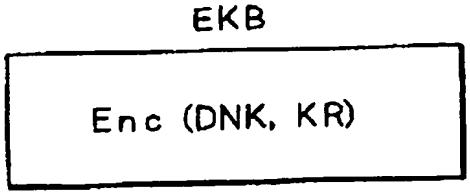

EKB
Enc (DNK, KR)

图 20

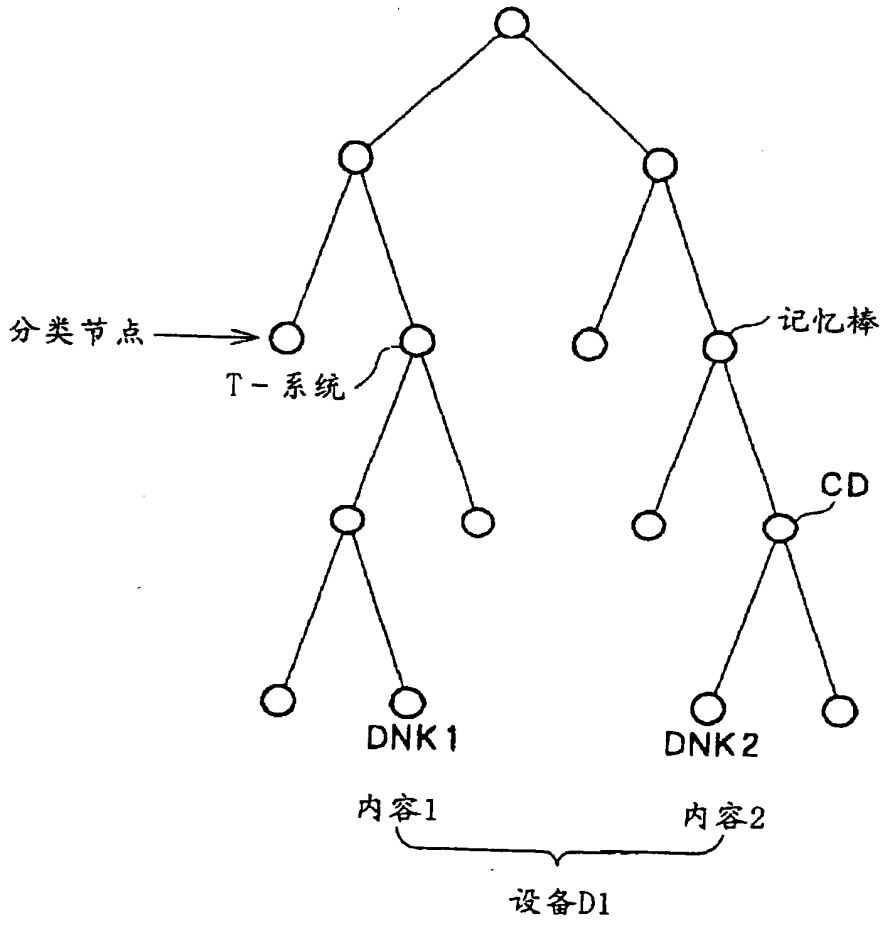


图 21

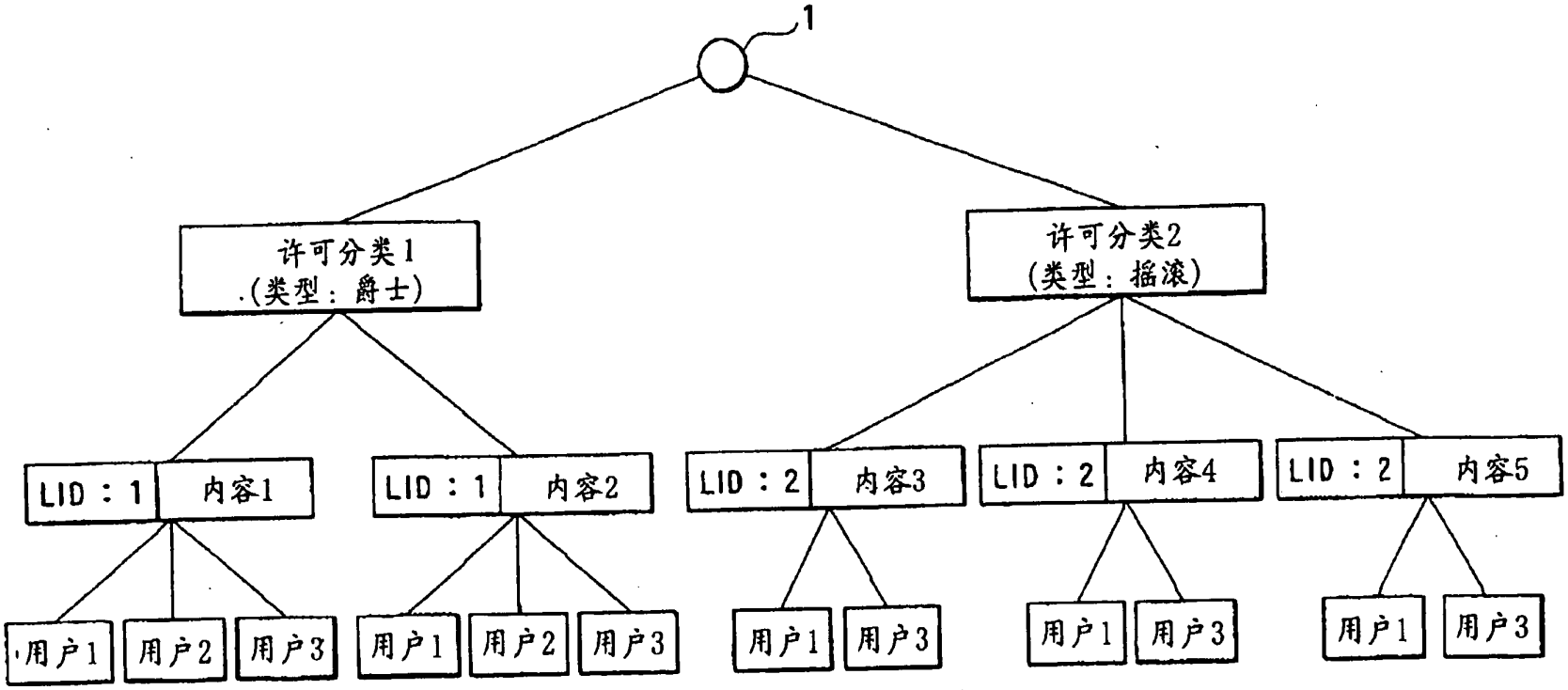

1
许可分类1
(类型：爵士)
许可分类2
(类型：摇滚)
LID：1
内容1
LID：1
内容2
LID：2
内容3
LID：2
内容4
LID：2
内容5
用户1
用户2
用户3
用户1
用户2
用户3
用户1
用户3
用户1
用户3
用户1
用户3

图 22

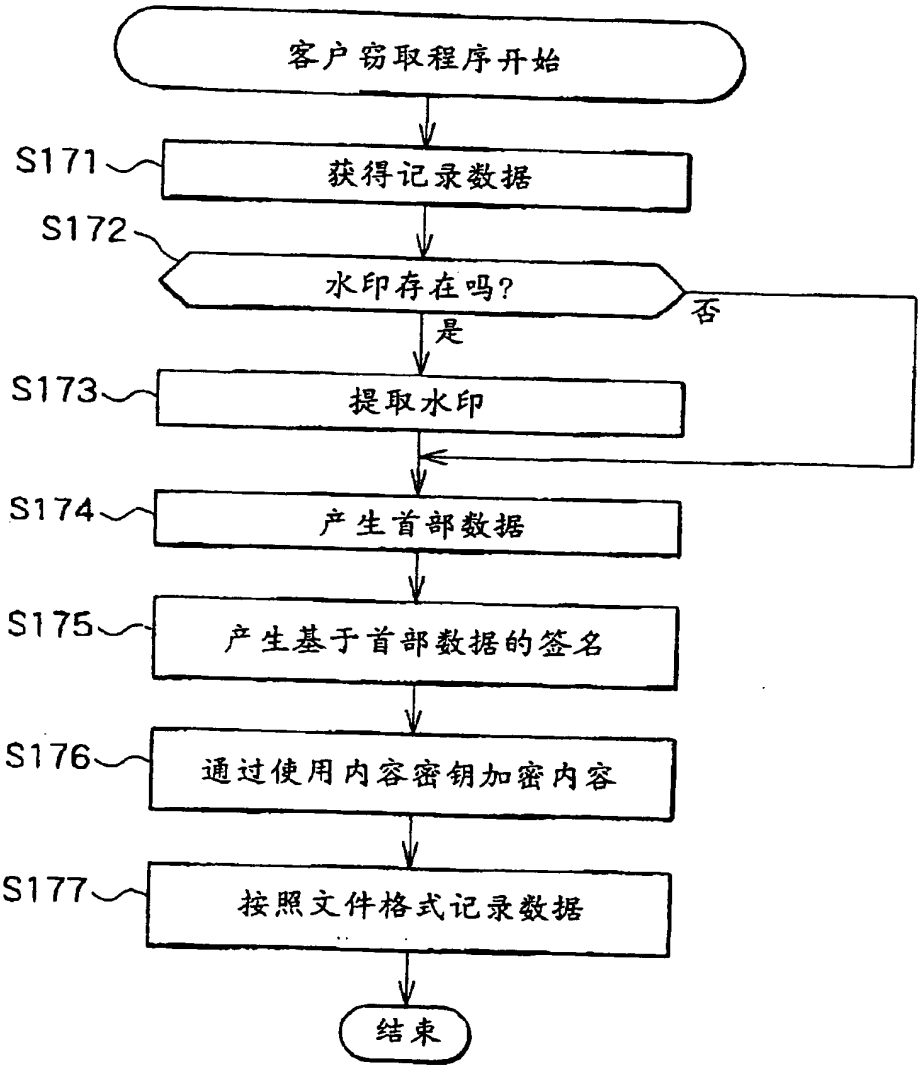

客户窃取程序开始
S171
获得记录数据
S172
水印存在吗?
否
是
S173
提取水印
S174
产生首部数据
S175
产生基于首部数据的签名
S176
通过使用内容密钥加密内容
S177
按照文件格式记录数据
结束

图 23

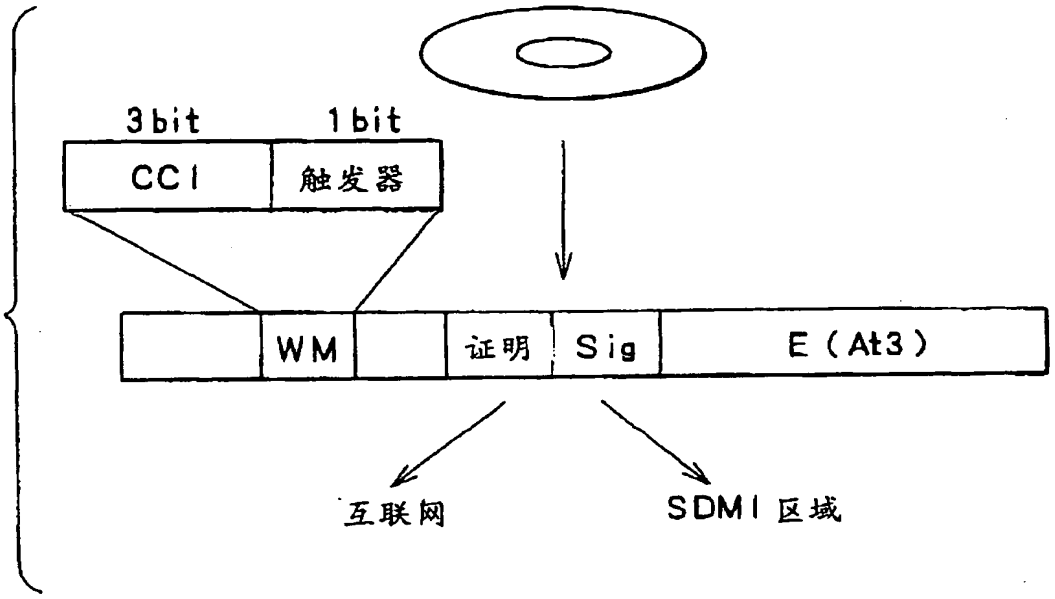

3bit
1bit
CCI
触发器
WM
证明
Sig
E（At3）
互联网
SDMI 区域

图 24

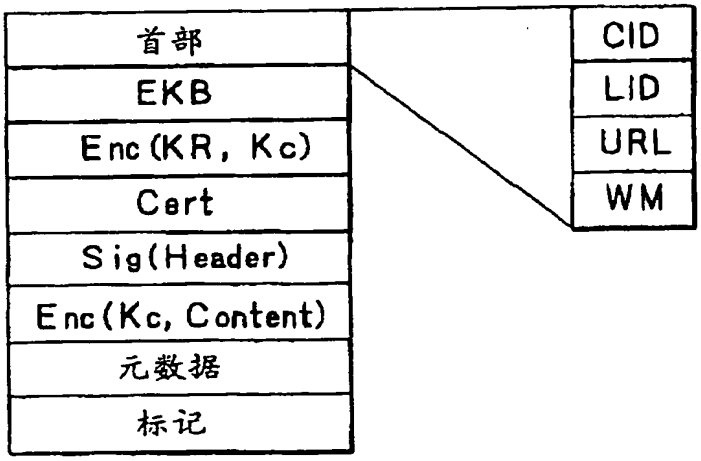

首部
EKB
Enc(KR, Kc)
Cert
Sig(Header)
Enc(Kc, Content)
元数据
标记
CID
LID
URL
WM

图 25

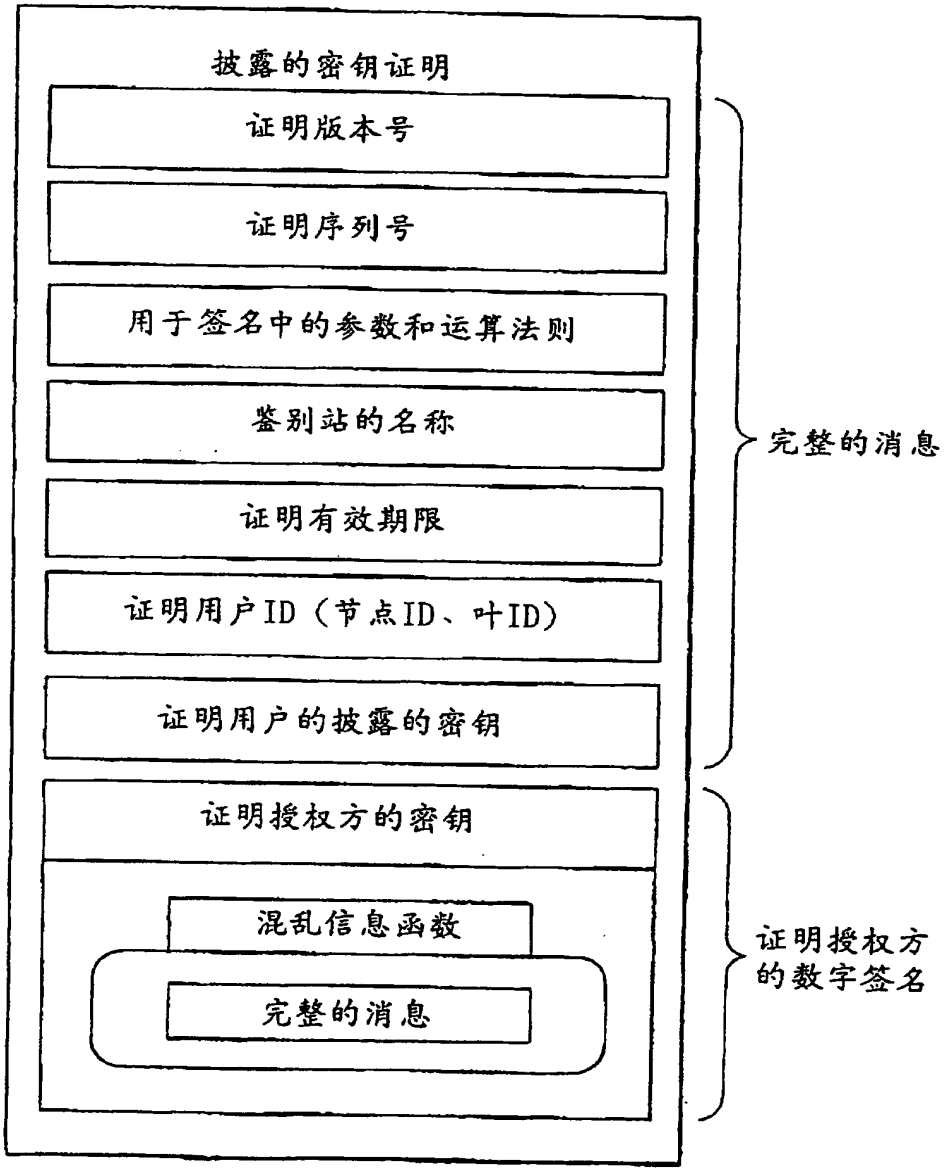

披露的密钥证明
证明版本号
证明序列号
用于签名中的参数和运算法则
鉴别站的名称
证明有效期限
证明用户ID（节点ID、叶ID）
证明用户的披露的密钥
证明授权方的密钥
混乱信息函数
完整的消息
完整的消息
证明授权方的数字签名

图 26

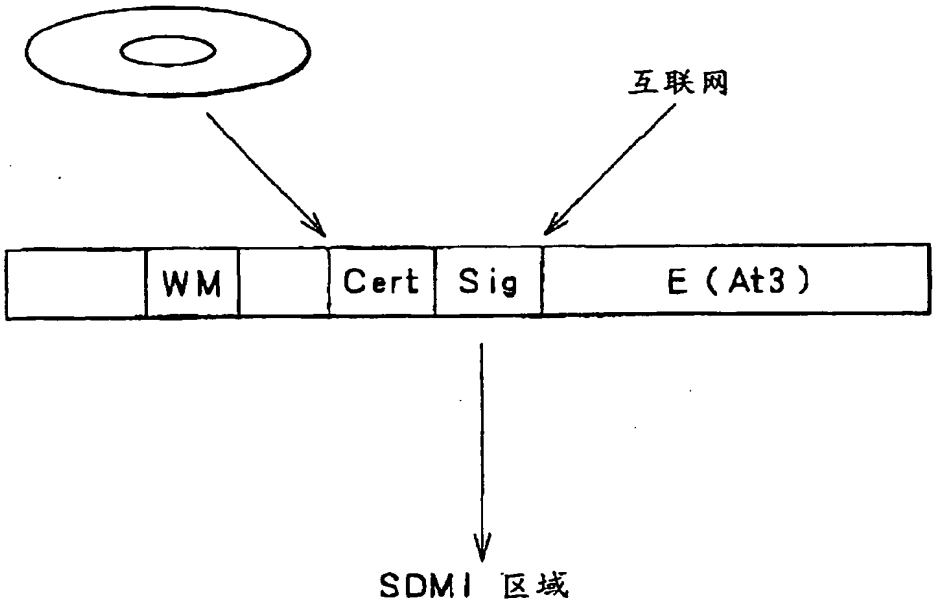


图 27

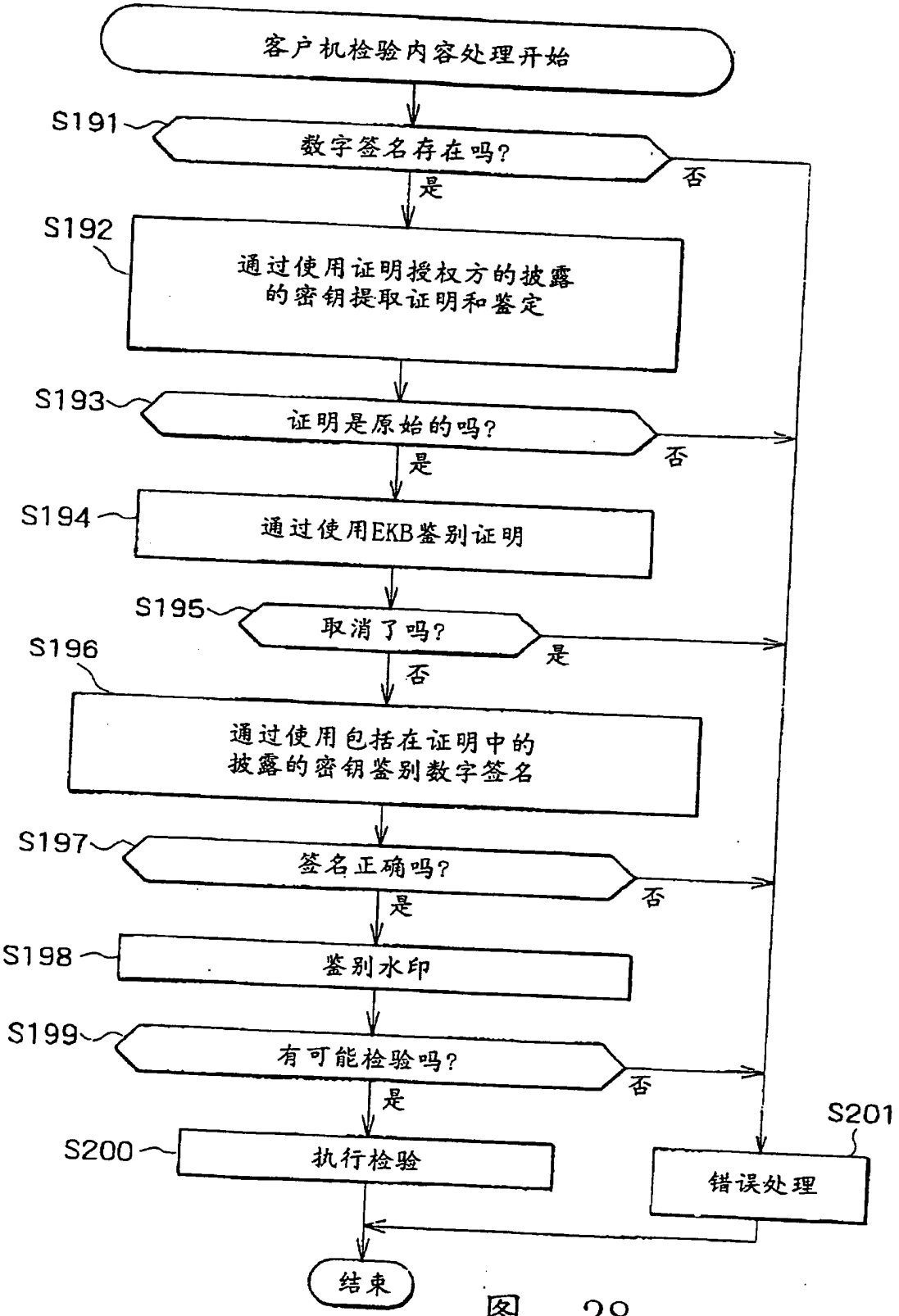

客户机检验内容处理开始
S191
数字签名存在吗?
否
是
S192
通过使用证明授权方的披露的密钥提取证明和鉴定
S193
证明是原始的吗?
否
是
S194
通过使用EKB鉴别证明
S195
取消了吗?
是
否
S196
通过使用包括在证明中的披露的密钥鉴别数字签名
S197
签名正确吗?
否
是
S198
鉴别水印
S199
有可能检验吗?
否
是
S200
执行检验
S201
错误处理
结束

图 28

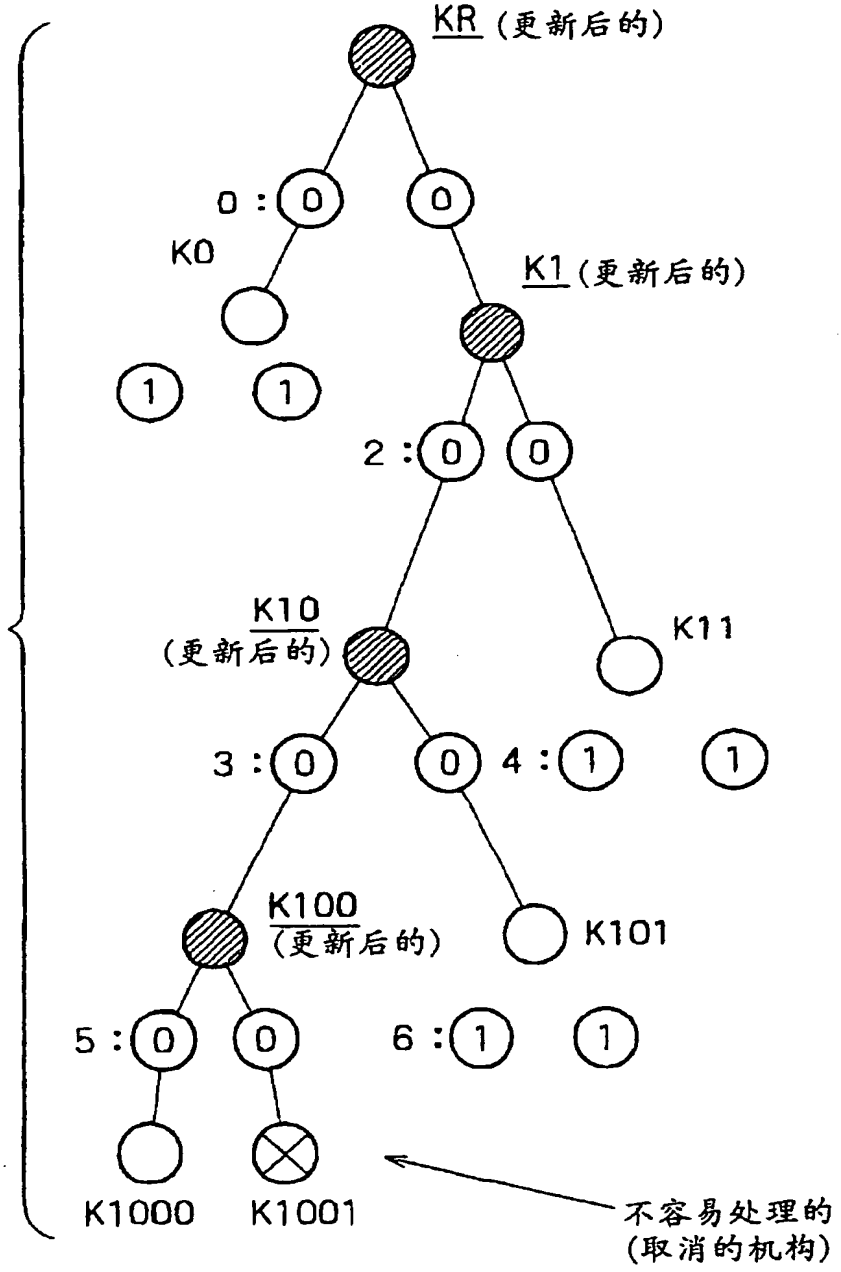

KR (更新后的)
0 : 0
0
K0
K1 (更新后的)
1
1
2 : 0
0
K10
(更新后的)
K11
3 : 0
0
4 : 1
1
K100
(更新后的)
K101
5 : 0
0
6 : 1
1
K1000
K1001
不容易处理的
(取消的机构)

图 29

EKB的数据部分和标记
(使能密钥块)

数据 (加密的密钥)	Enc(K0, K(t)R, Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1), Enc(K11, K(t)1) Enc(K(t)100, K(t)10), Enc(K101, K(t)10) Enc(K1000, K(t)100)
标记	0:{0,0}, 1:{1,1}, 2:{0,0}, 3:{0,0} 4:{1,1}, 5:{0,1}, 6:{1,1}

{L 标记 , R 标记 }

L标记和R标记每个0表示存在数据,
而1表示不存在数据

图 30

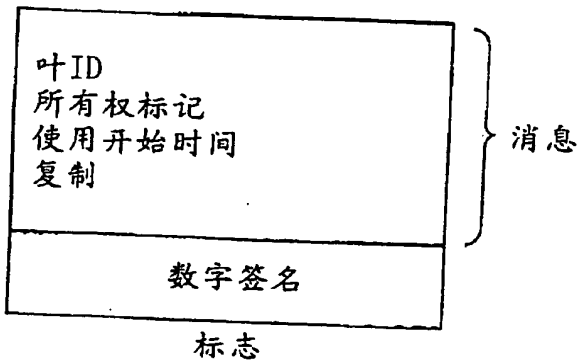


图 31

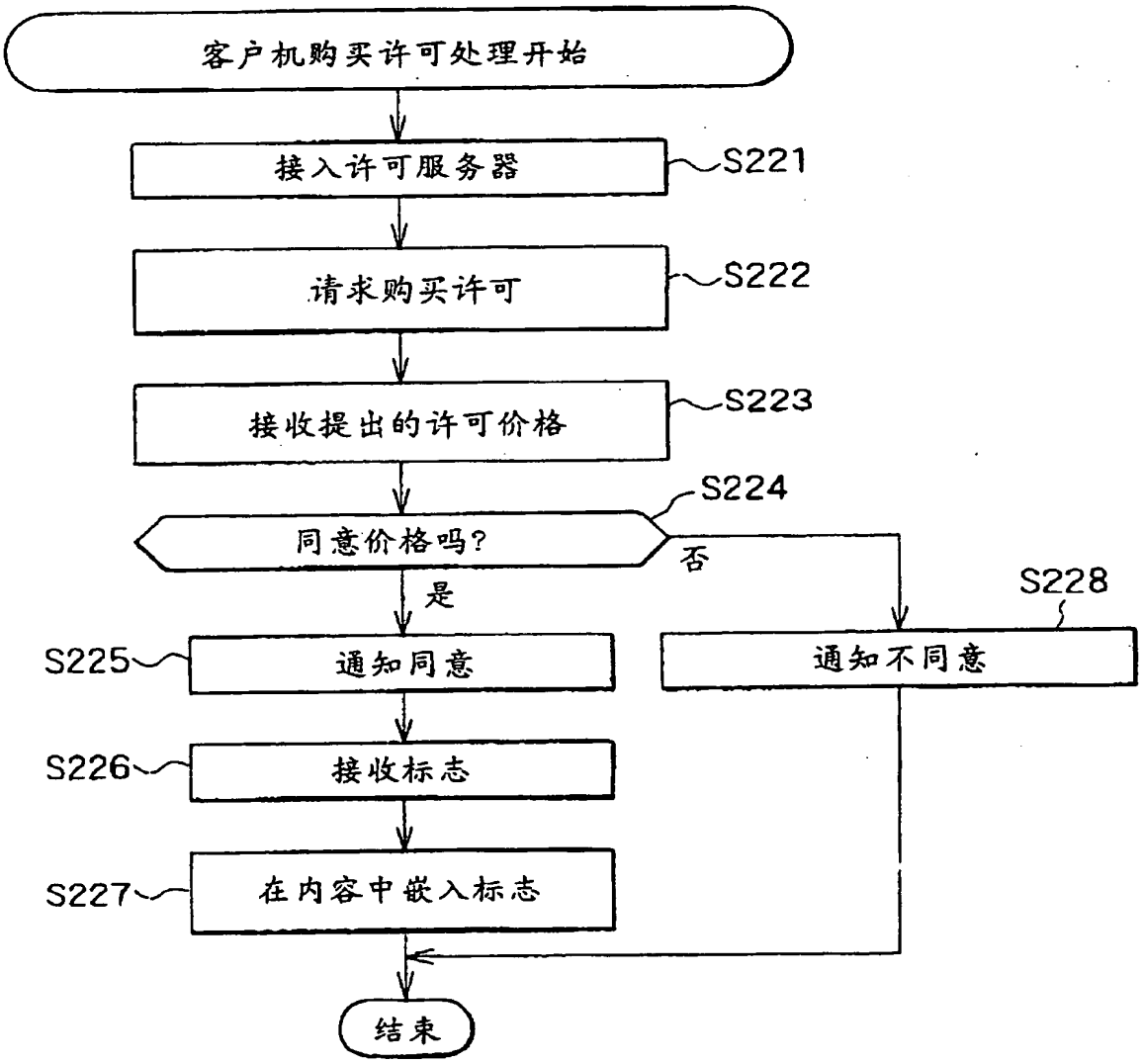

客户机购买许可处理开始
接入许可服务器
S221
请求购买许可
S222
接收提出的许可价格
S223
S224
同意价格吗?
否
是
S228
S225
通知同意
通知不同意
S226
接收标志
S227
在内容中嵌入标志
结束

图 32

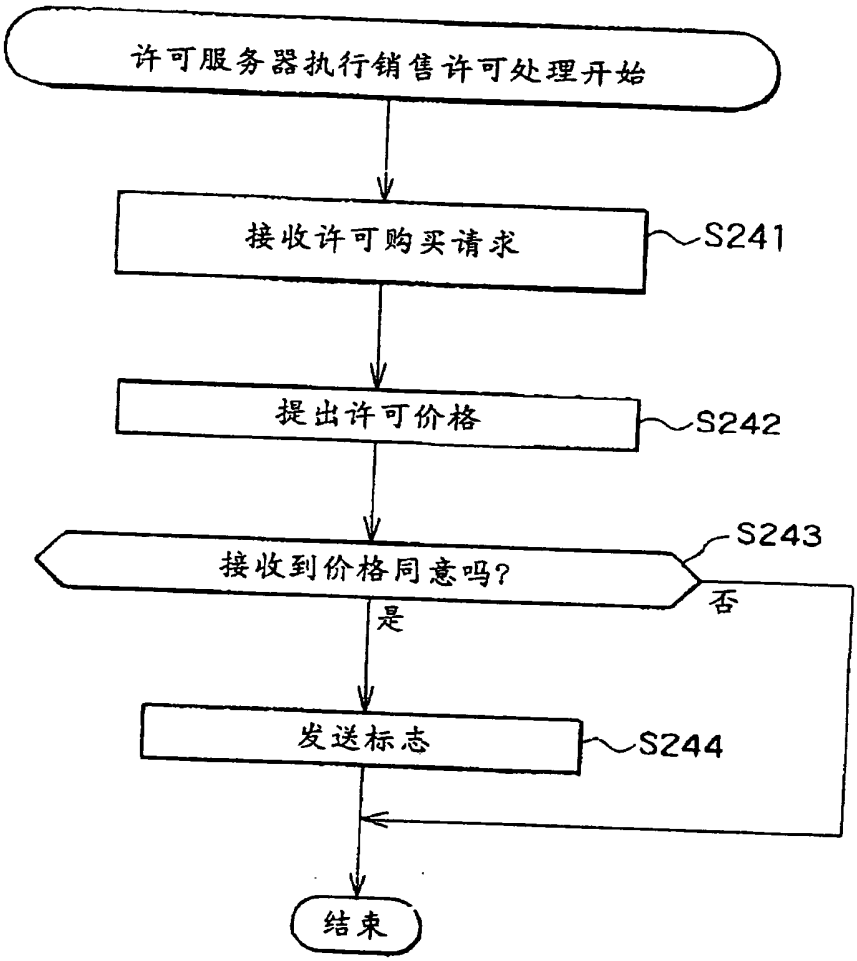

许可服务器执行销售许可处理开始
接收许可购买请求
S241
提出许可价格
S242
接收到价格同意吗?
S243
否
是
发送标志
S244
结束

图 33

标志 = { 叶 ID, Own, Sig_S(叶 ID, Own)}

图 34

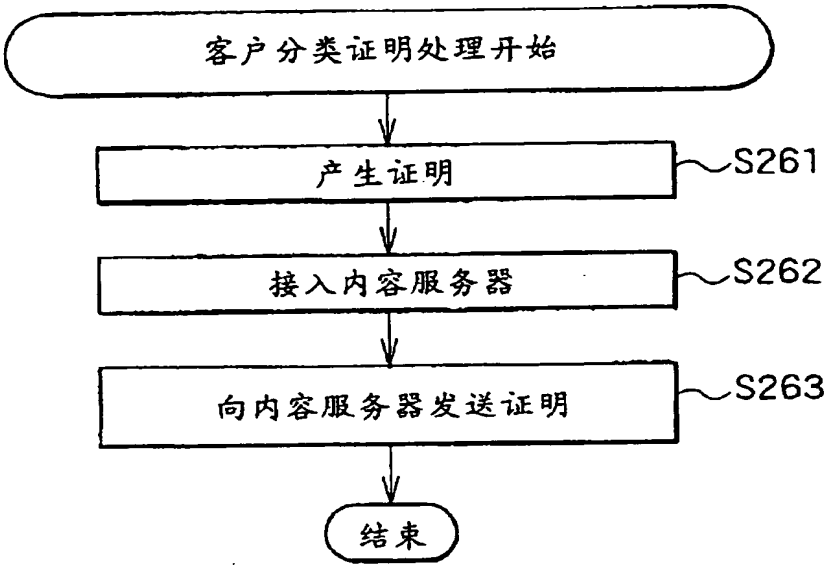


图 35

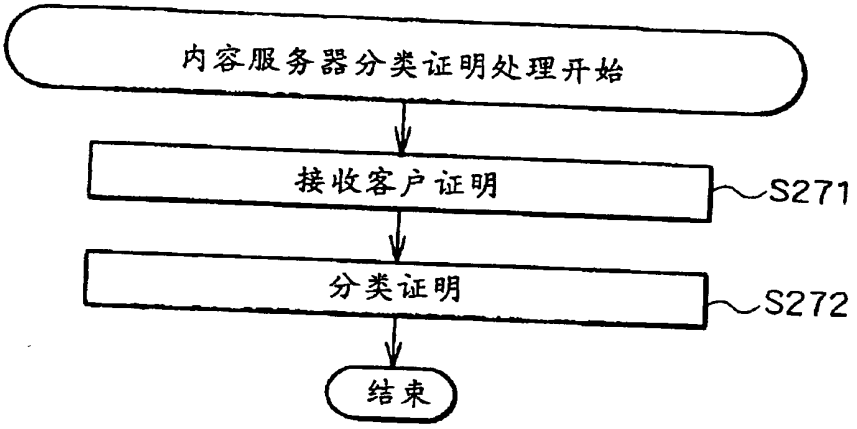

内容服务器分类证明处理开始
接收客户证明
S271
分类证明
S272
结束

图 36

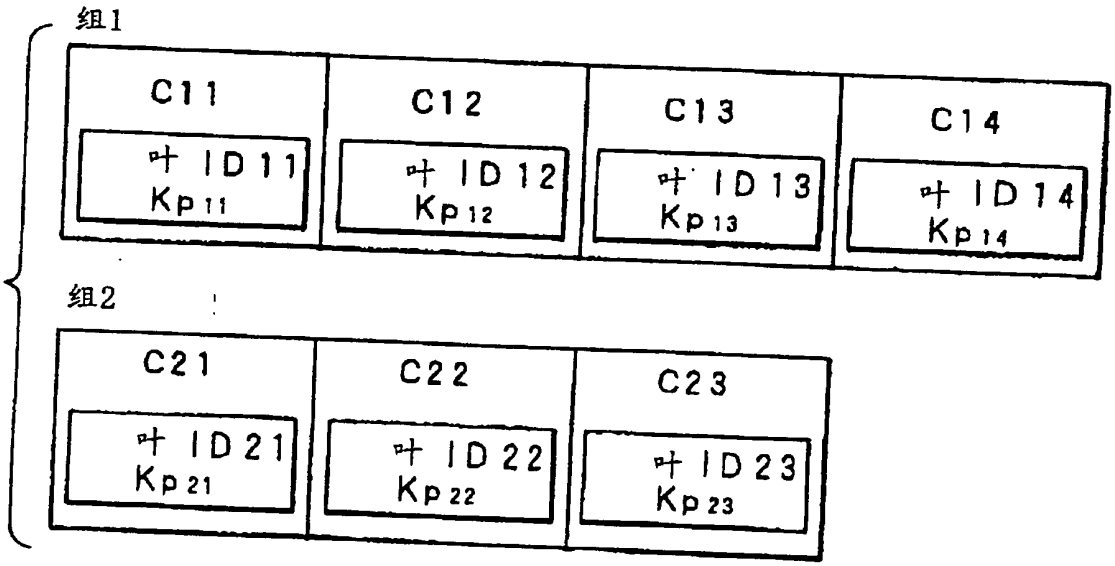

组1
C11
叶 ID11
Kp11
C12
叶 ID12
Kp12
C13
叶 ID13
Kp13
C14
叶 ID14
Kp14
组2
C21
叶 ID21
Kp21
C22
叶 ID22
Kp22
C23
叶 ID23
Kp23

图 37

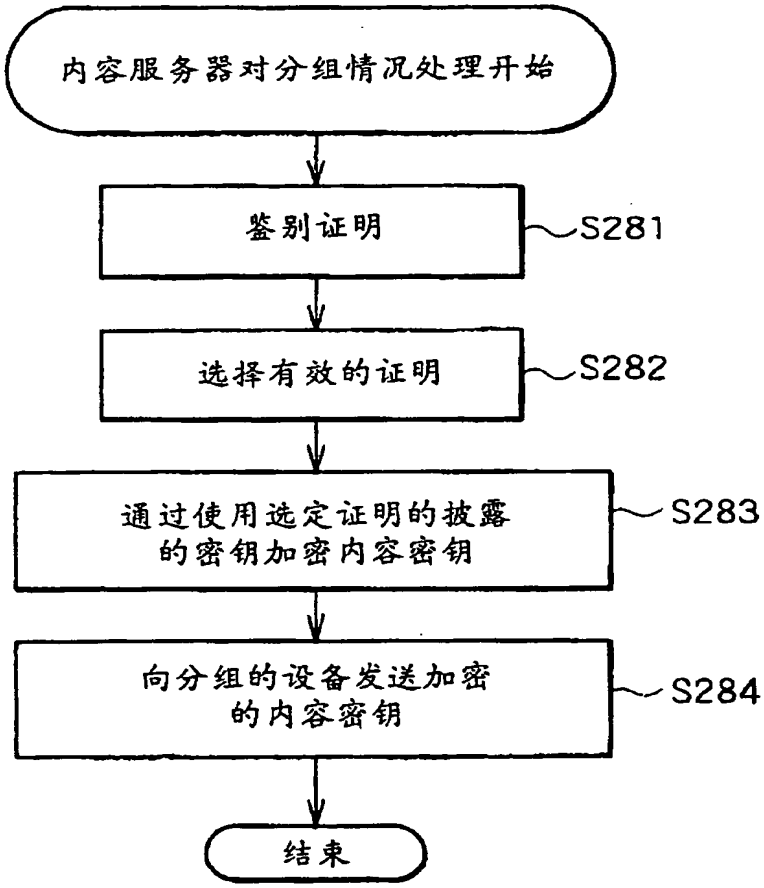


图 38

Enc(Kp11, Kc), Enc(Kp12, Kc), Enc(Kp13, Kc)

图 39

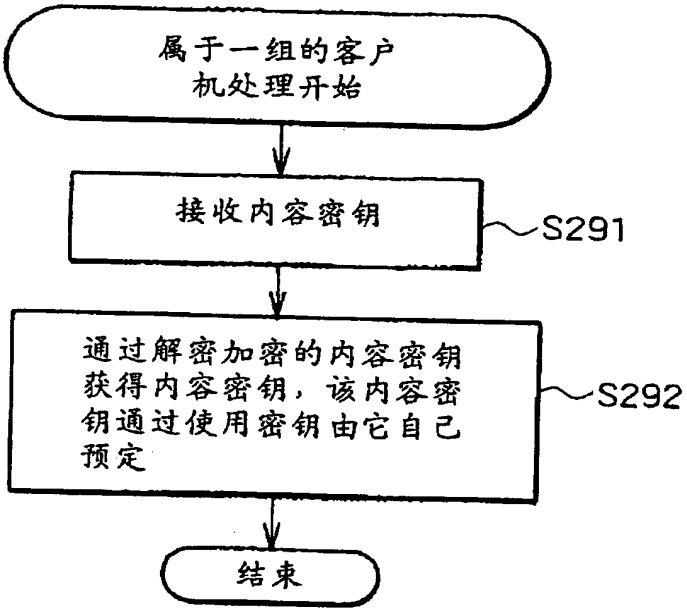

属于一组的客户机处理开始
接收内容密钥
S291
通过解密加密的内容密钥获得内容密钥，该内容密钥通过使用密钥由它自己预定
S292
结束

图 40

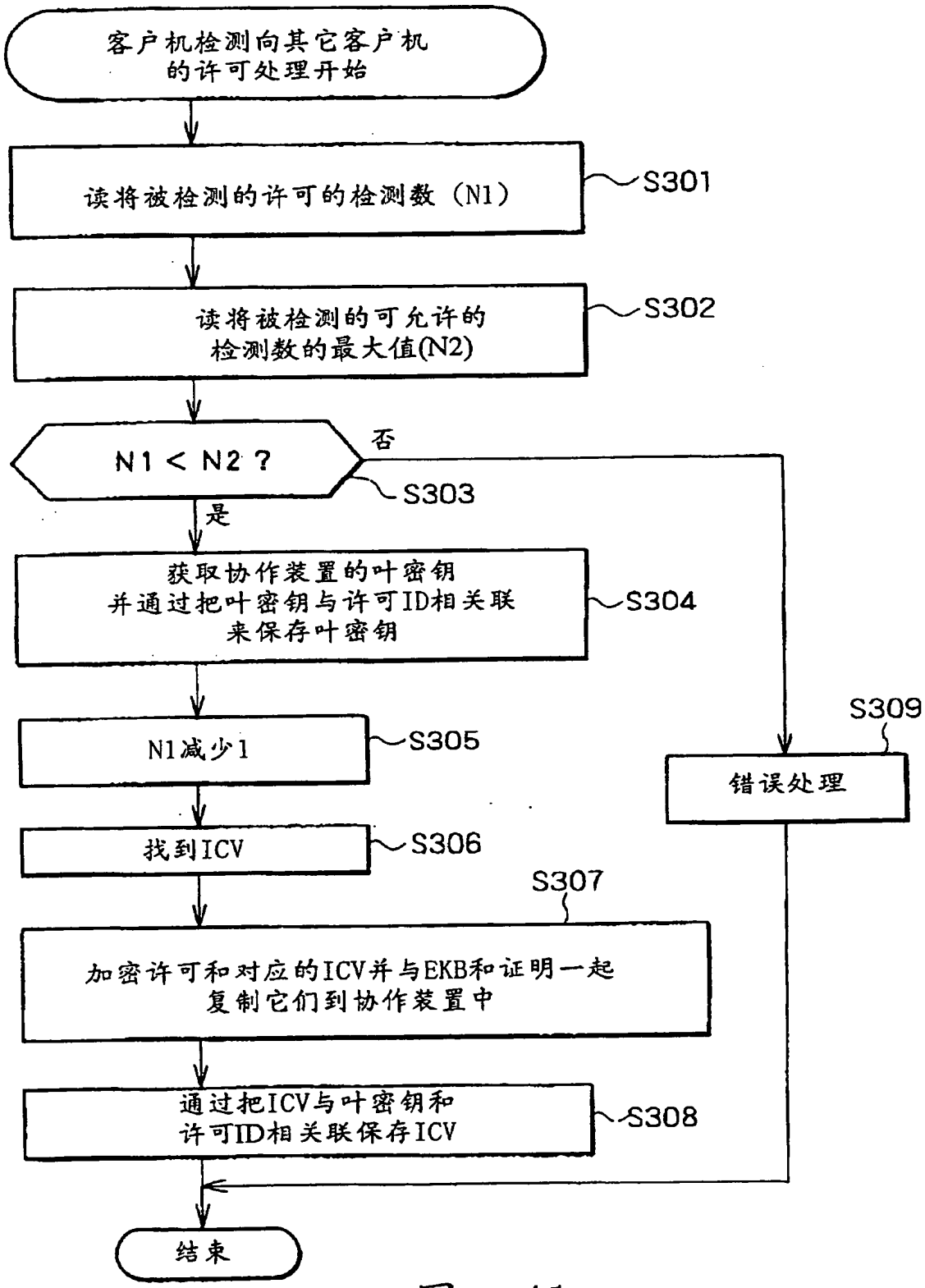

客户机检测向其它客户机
的许可处理开始
读将被检测的许可的检测数（N1）
S301
读将被检测的可允许的
检测数的最大值(N2)
S302
N1 < N2 ?
否
S303
是
获取协作装置的叶密钥
并通过把叶密钥与许可ID相关联
来保存叶密钥
S304
N1减少1
S305
找到ICV
S306
S307
加密许可和对应的ICV并与EKB和证明一起
复制它们到协作装置中
通过把ICV与叶密钥和
许可ID相关联保存ICV
S308
S309
错误处理
结束

图 41

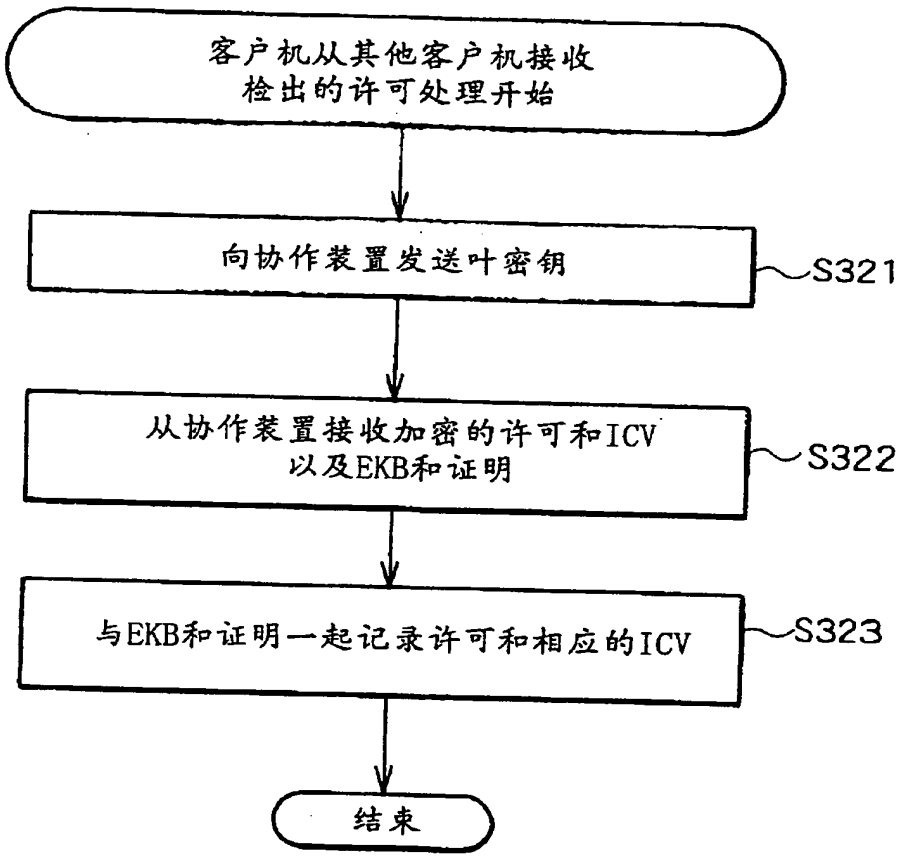

客户机从其他客户机接收
检出的许可处理开始
向协作装置发送叶密钥
S321
从协作装置接收加密的许可和ICV
以及EKB和证明
S322
与EKB和证明一起记录许可和相应的ICV
S323
结束

图 42

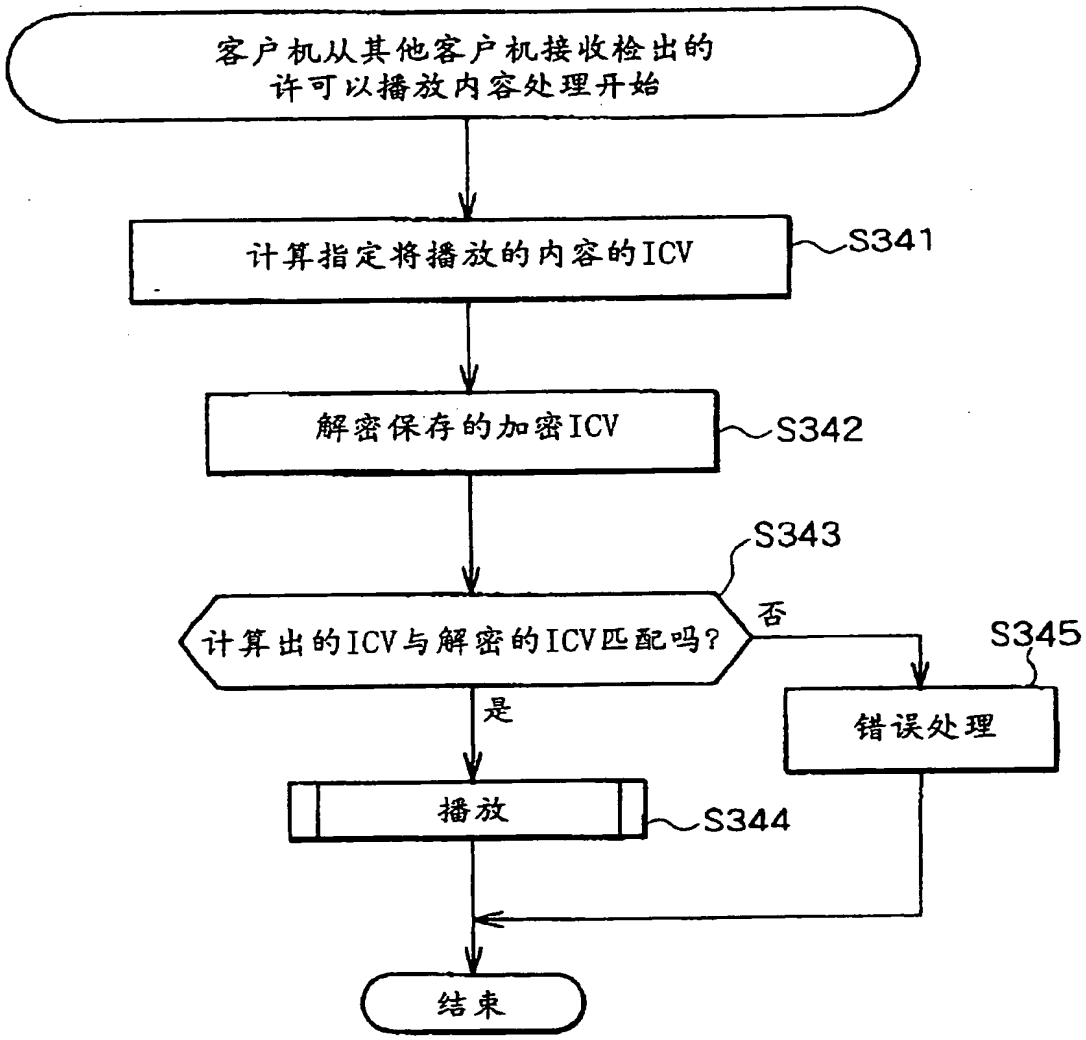

客户机从其他客户机接收检出的
许可以播放内容处理开始
计算指定将播放的内容的ICV
S341
解密保存的加密ICV
S342
S343
计算出的ICV与解密的ICV匹配吗?
否
S345
是
错误处理
播放
S344
结束

图 43

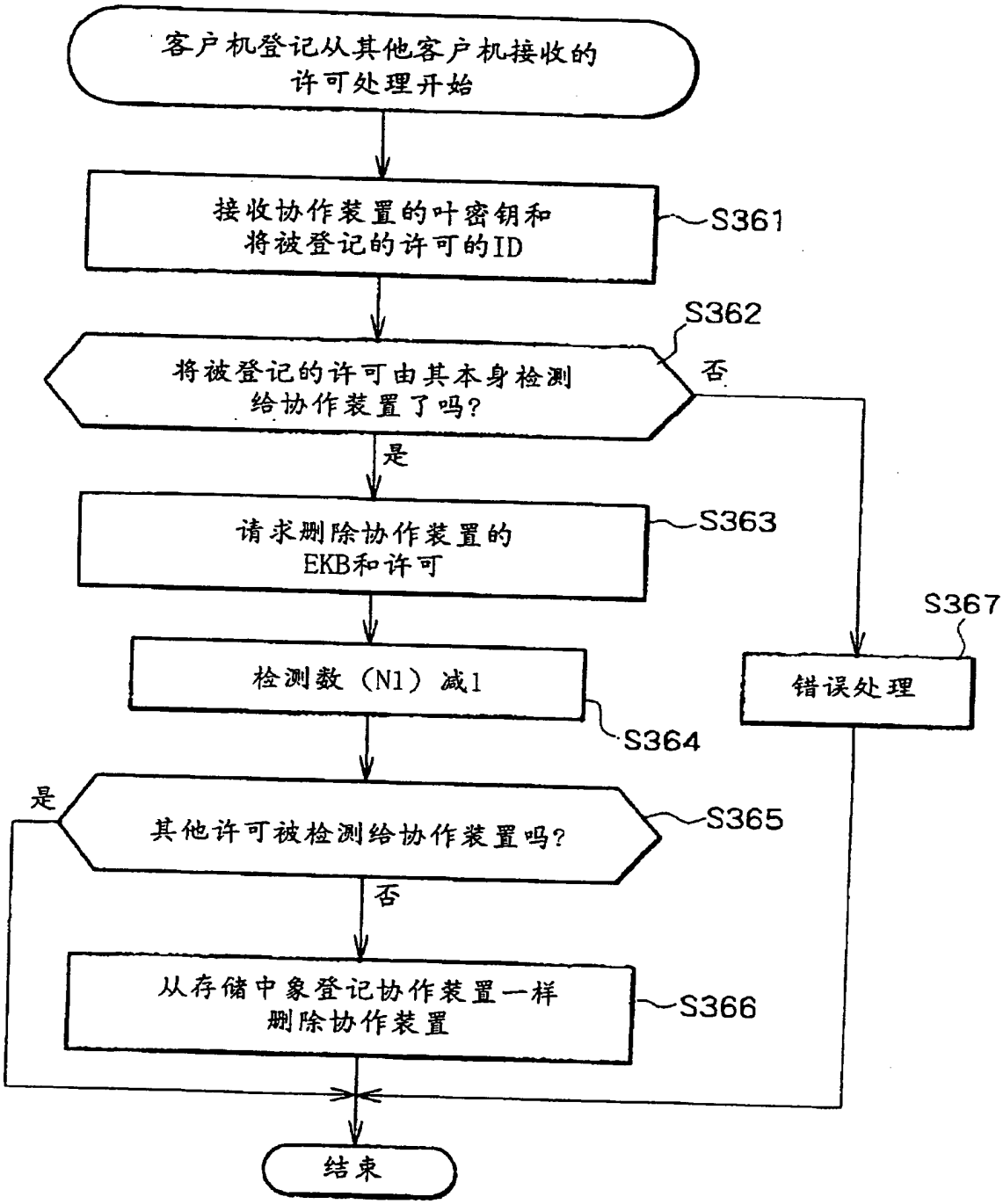

客户机登记从其他客户机接收的
许可处理开始
接收协作装置的叶密钥和
将被登记的许可的ID
S361
S362
将被登记的许可由其本身检测
给协作装置了吗?
否
是
请求删除协作装置的
EKB和许可
S363
S367
检测数（N1）减1
S364
错误处理
是
其他许可被检测给协作装置吗?
S365
否
从存储中象登记协作装置一样
删除协作装置
S366
结束

图 44

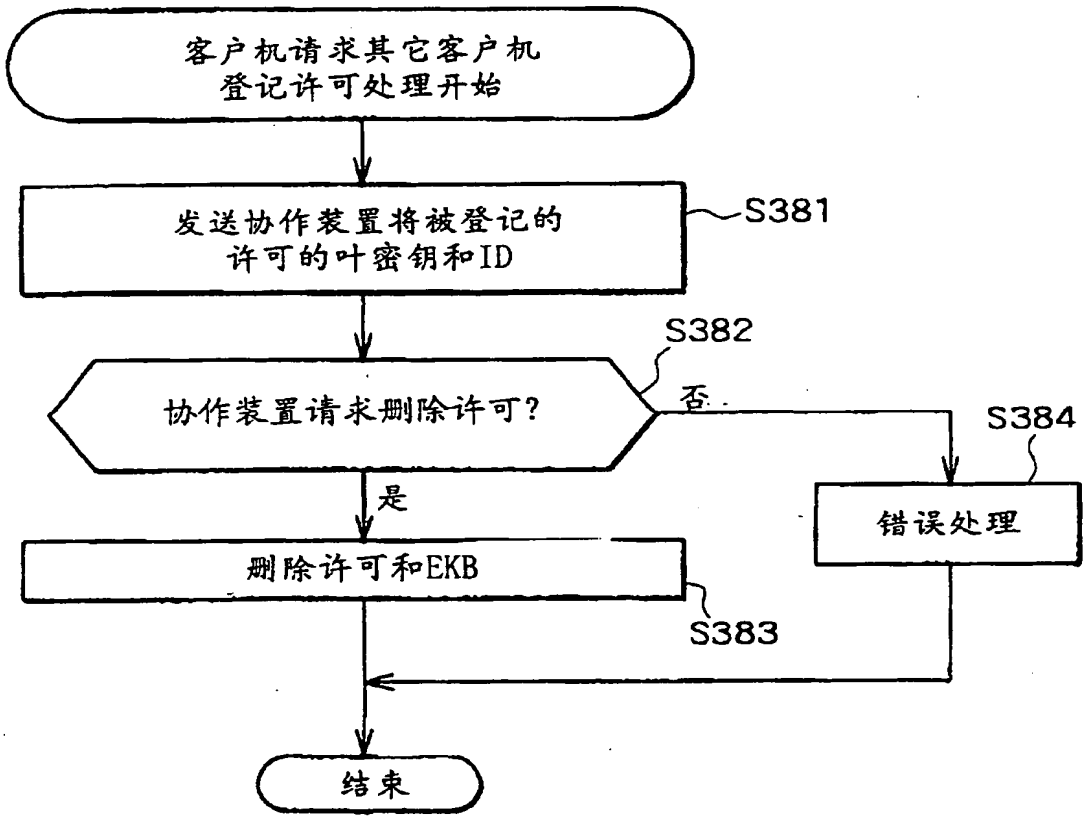

客户机请求其它客户机
登记许可处理开始
发送协作装置将被登记的
许可的叶密钥和ID
S381
S382
协作装置请求删除许可?
否
S384
是
错误处理
删除许可和EKB
S383
结束

图 45

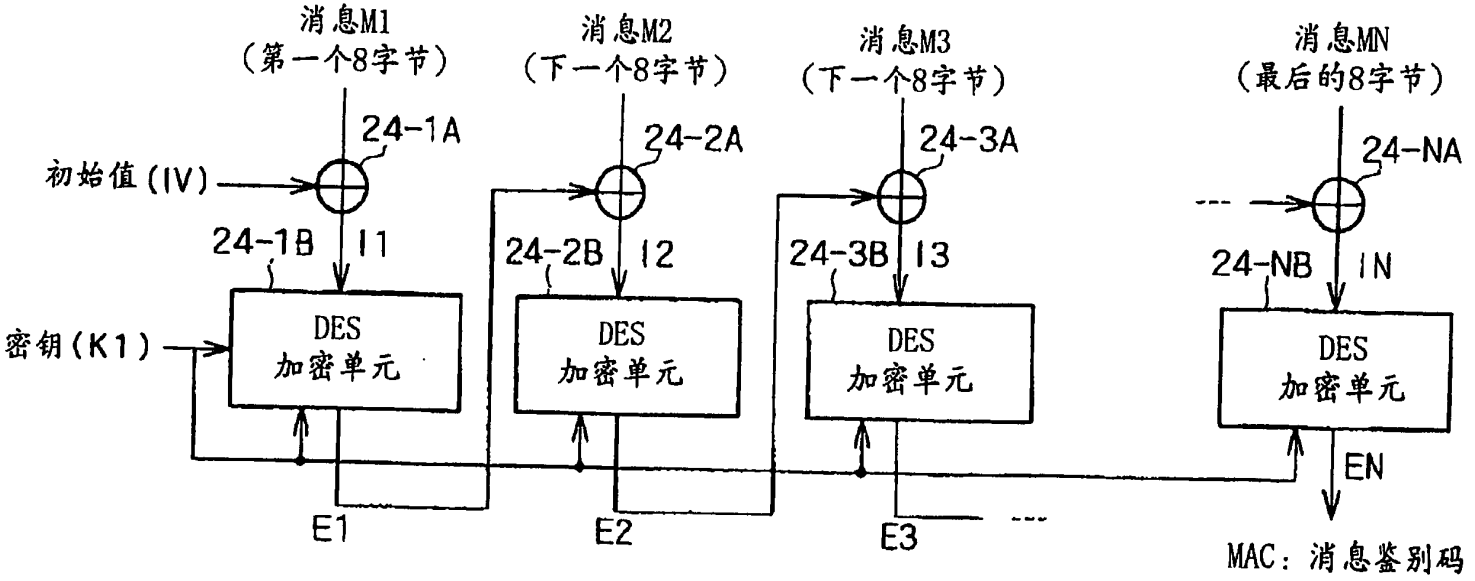

消息M1
（第一个8字节）
消息M2
（下一个8字节）
消息M3
（下一个8字节）
消息MN
（最后的8字节）
24-1A
24-2A
24-3A
24-NA
初始值(IV)
24-1B
I1
24-2B
I2
24-3B
I3
24-NB
IN
密钥(K1)
DES
加密单元
DES
加密单元
DES
加密单元
DES
加密单元
EN
E1
E2
E3
MAC：消息鉴别码
⊕：专用的逻辑和处理（以8字节为单位）

图 46

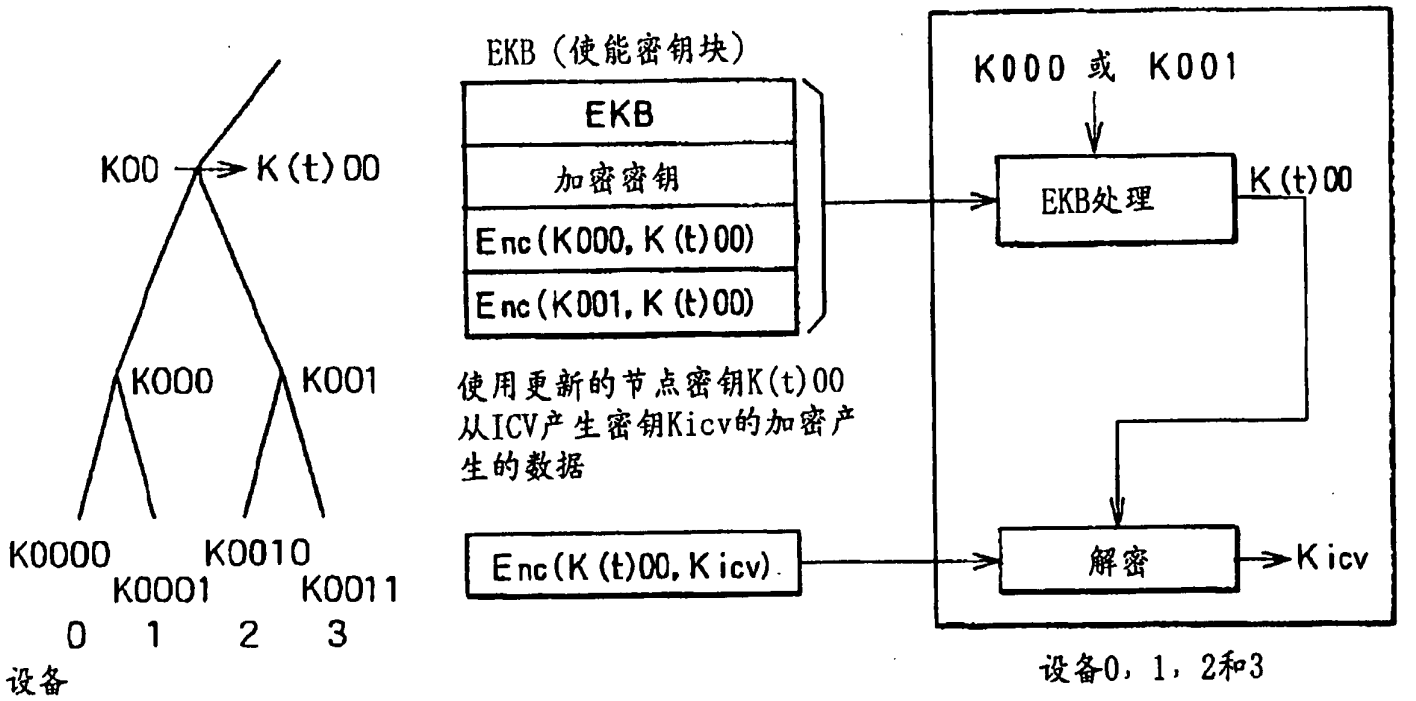

K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
设备
EKB（使能密钥块）
EKB
加密密钥
Enc(K000, K(t)00)
Enc(K001, K(t)00)
使用更新的节点密钥K(t)00
从ICV产生密钥Kicv的加密产
生的数据
Enc(K(t)00, Kicv)
K000 或 K001
EKB处理
K(t)00
解密
Kicv
设备0，1，2和3

图 47

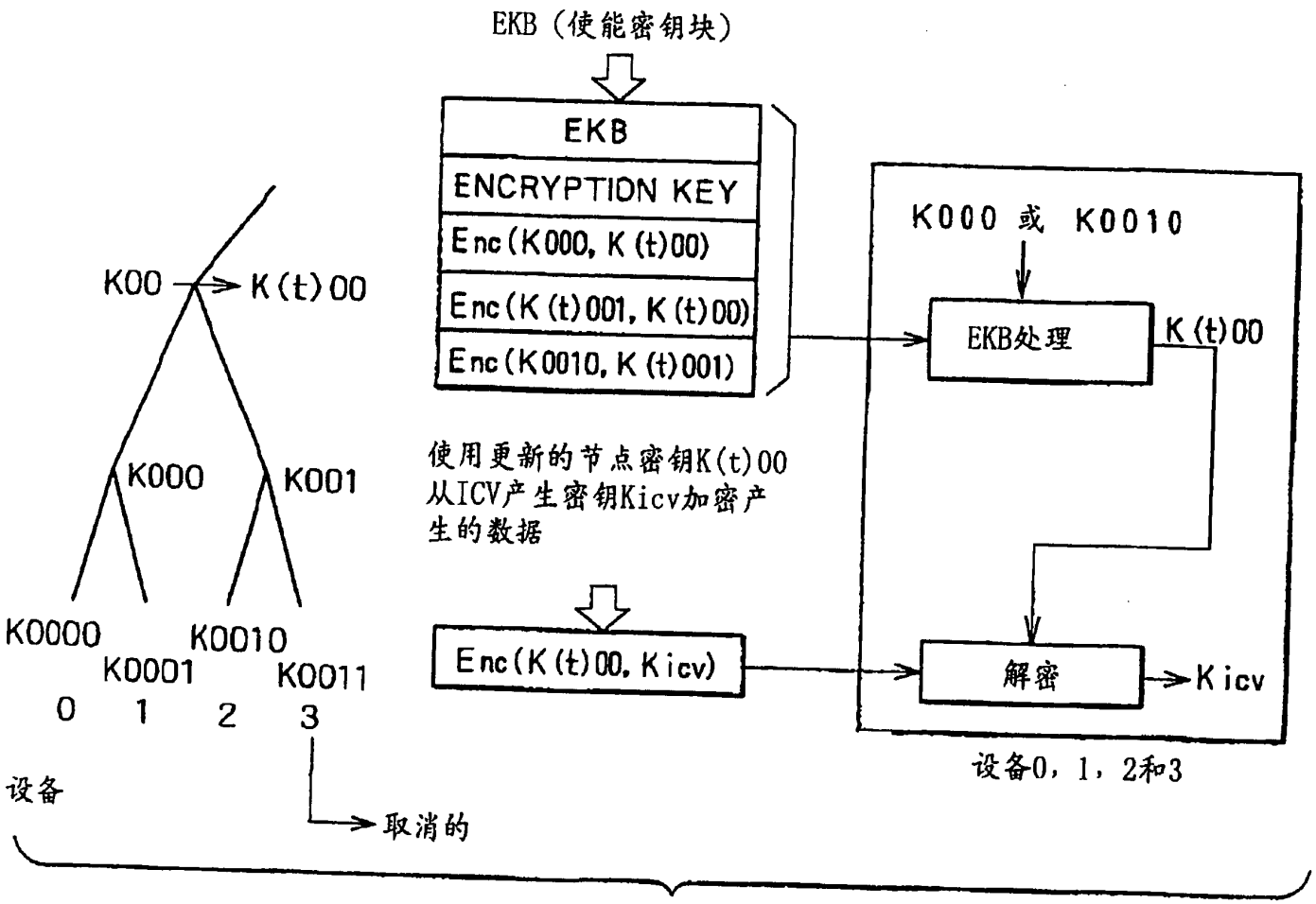

EKB（使能密钥块）
EKB
ENCRYPTION KEY
Enc(K000, K(t)00)
Enc(K(t)001, K(t)00)
Enc(K0010, K(t)001)
K00
K(t)00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
设备
取消的
使用更新的节点密钥K(t)00
从ICV产生密钥Kicv加密产
生的数据
Enc(K(t)00, Kicv)
K000 或 K0010
EKB处理
K(t)00
解密
Kicv
设备0，1，2和3

图 48

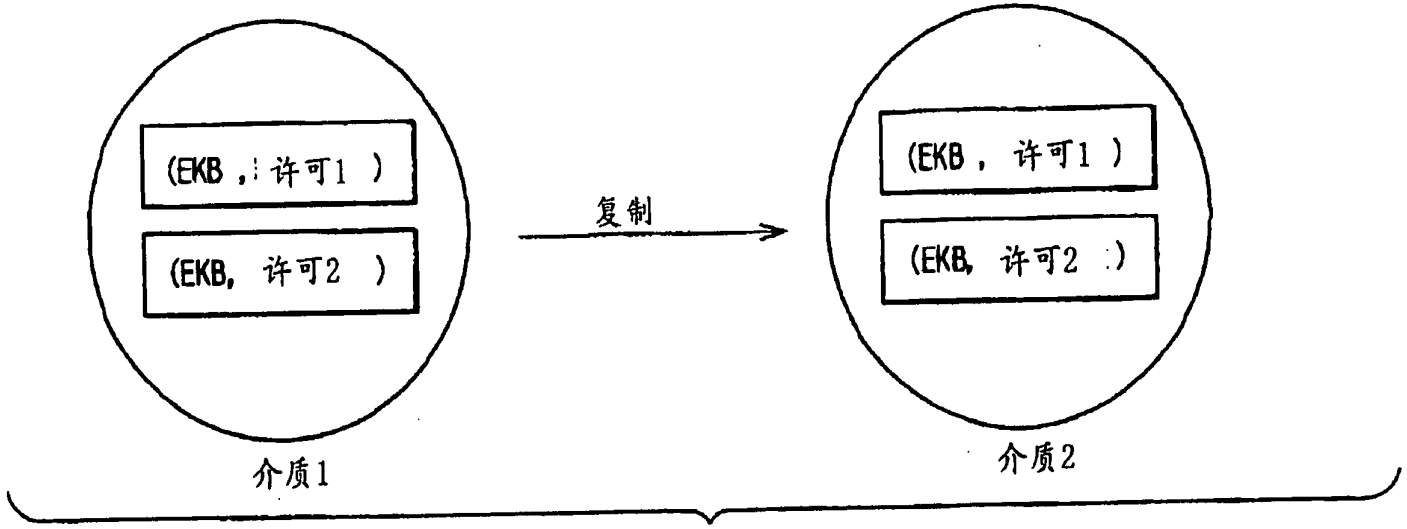

(EKB，许可1)
(EKB, 许可2)
复制
(EKB，许可1)
(EKB, 许可2)
介质1
介质2

图 49A

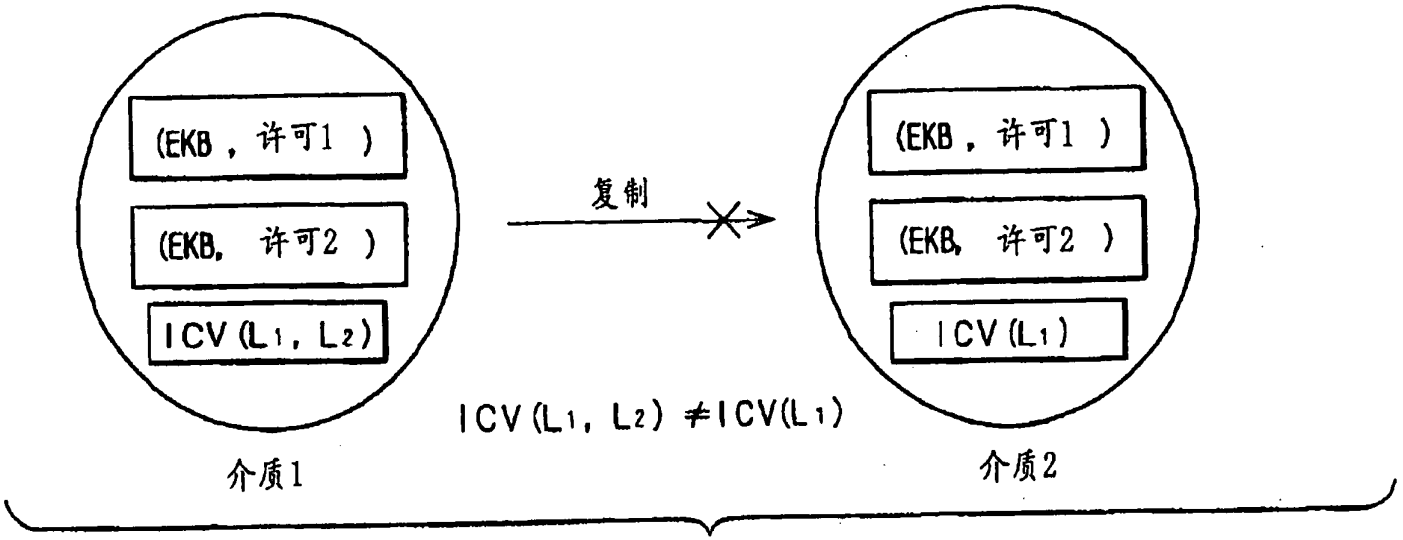

(EKB，许可1)
(EKB, 许可2)
ICV (L1, L2)
复制
(EKB，许可1)
(EKB, 许可2)
ICV (L1)
ICV (L1, L2) ≠ICV(L1)
介质1
介质2

图 49B

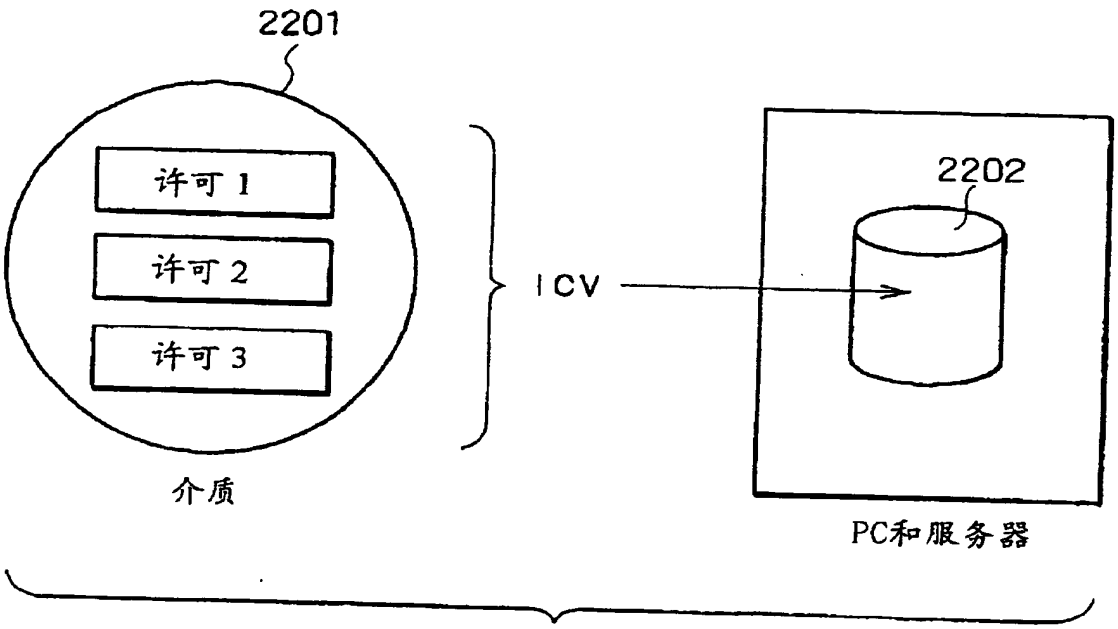


图 50